NATIONAL SECURITY AGENCY
CYBERSECURITY INFORMATION

# DEFEND PRIVILEGES AND ACCOUNTS

## KEYS TO THE KINGDOM

A typical enterprise network contains many high value items, or assets. These assets could be information—corporate knowledge or intellectual property. They could be capabilities—the ability to control equipment or processes, to transfer funds, or to approve actions. Malicious actors steal this information for profit, threaten the destruction of the information for extortion (i.e. ransomware), and abuse capabilities to misuse, destroy, or degrade service. Often, they do this by exploiting poorly defended privileges and accounts. Stolen account credentials and the use of legitimate privileges allow an adversary to avoid using malware, which can leave telltale artifacts.

Privileges are rights granted to an individual, program, or process, sometimes expressed as an action that a user is permitted to perform on an asset [1]. They are sometimes as simple as the ability to read or modify a file, to access a database, or to log on to a corporate server. An account is a set of privileges given to an authenticated entity, usually a user. For example, a user might be given an administrative account on a device with privileges to log on, install new programs, and access the file system. While administrative privileges are typically unavailable to most users, both administrative and non-administrative accounts must be safeguarded.

Threats of credential misuse come from actors outside the organization as well as inside. The Verizon 2018 Data Breach Investigation Report named stolen credentials, phishing, and privilege abuse as three of the top five action varieties observed in breaches that year [2]. By identifying and ranking assets, controlling the accounts that allow access to those assets, strongly authenticating the users of those accounts, and monitoring how those accounts are used, an enterprise improves its ability to protect its most valuable assets.

## THE LIFECYCLE

Account and privilege defense is a continual process. System owners constantly review accounts and their associated risks. Thoroughly documenting each phase of the lifecycle—identify, protect, and monitor—provides a reference for consistency, continuity, and understanding. Adherence to organizational policies ensure that the documentation and practices comply with legal standards and obligations.

### Identify assets, users, and accounts

Discovering the organization's high value assets and ranking them based on their associated risks to operations identifies the areas where defenses need to be prioritized. Typically the highest value assets are correlated with the greatest risk to mission success or business continuity.

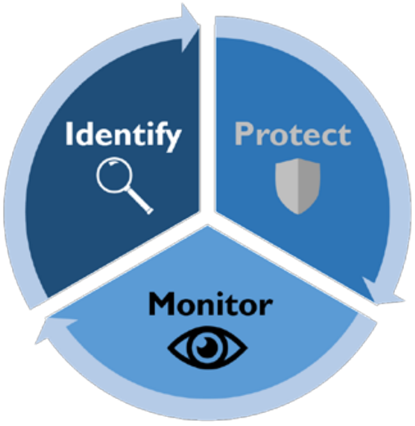

Figure 1: DP&A Lifecycle

The next step is to identify all the privileges and accounts associated with each asset and to rank these privileges and accounts based on the risk or exposure the privileges and accounts pose to the asset. When identifying accounts and privileges an organization considers the following questions [3]:

- What tasks require privileges over this asset?
- How many accounts need privileges over the asset to complete each task and for how long?
- Are there currently privileges or accounts for this asset that are not associated with a task?
- Do privileges and accounts for this asset inadvertently give the user privileges and accounts for other assets?
- Which of these privileges and accounts have administrative capabilities?

Traditionally, administrative accounts have been the biggest targets, because these accounts typically have access to all the assets in the network, but user accounts may also have access to high value assets. For instance, executive user accounts may have access to valuable data.

## Protect accounts

The mechanisms of access control, least privilege, and authentication, when implemented together, integrate to protect accounts.

Protect accounts

Control access

Enforce least privilege

Require authentication

**Access Control** is the process of managing and enforcing the privileges that are assigned to accounts. Providing functional separation of assets can ease the establishment and maintenance of access controls. Segregation of a network through physical or logical means separates functions that have minimal or no interaction.[1] When done correctly, network segmentation can hinder certain types of lateral movement and limit the potential damage from an attack or breach. For systems employing directories for access control, this may require separating user groups and administration of those user groups, in addition to controlling the flow of network traffic.

**Least privilege** is the restriction of privileges to only those accounts that require them to perform their duties, while limiting accounts to only those privileges that are truly necessary. Doing this reduces the exposure of those privileges to a smaller, more easily manageable set of accounts. Local administrative accounts and accounts for software program management and installation are particularly powerful, but have small scopes of control and should be restricted as much as possible.

Having separate accounts for routine and sensitive activities further reduces privilege exposure. Privileged accounts should not be used to perform general tasks such as accessing emails and browsing the Internet.[2] Email and Internet browsing activities are inherently dangerous because they involve processing untrusted information that is potentially malicious. If accounts with high value privileges are used to perform these activities, a compromise can lead to immediate attacker control of those privileges. For these reasons, administrative and non-administrative privileges should be assigned to separate accounts for each user and asset. Additionally, on servers, disable or remove browsing and email capability altogether if not necessary for the server applications to function.

The principle of least privilege is particularly important when operating a Microsoft Active Directory®[3] (AD) domain, given the constant use of Pass-the-Hash (PtH) attacks by sophisticated actors and novices alike.

A tiered privilege architecture combined with strict access controls, such as Microsoft's Enhanced Security Administrative Environment (ESAE), implements the principle of least privilege across the AD infrastructure [4]. The ESAE reference architecture contains tiers of privileges. Each account is assigned to a tier based on the privileges and assets associated with the account. The highest level tier (Tier-0 in ESAE) contains the accounts that administer the access control system itself. Below that, there is a tier for administering enterprise services, and then for administering individual workstations and devices. Privilege restrictions and access controls are imposed at the tier level and restrict an account's privileges and access from the other administrative tiers. These layers of administrative access reduce the risk of privilege escalation by preventing the most critical credentials from being used or left on less critical systems. Tier based systems can be easier to manage than individual accounts.

[1] For more information on network segregation, please refer to *Segregate Networks Using Application Aware Defenses,* an NSA Cybersecurity Top 10 Mitigation document.

[2] For more information, please refer to *Enforcing No Internet or E-mail Access from Privileged Accounts*, MIT-003FS-2014.

[3] Active Directory is a registered trademark of Microsoft Corporation.

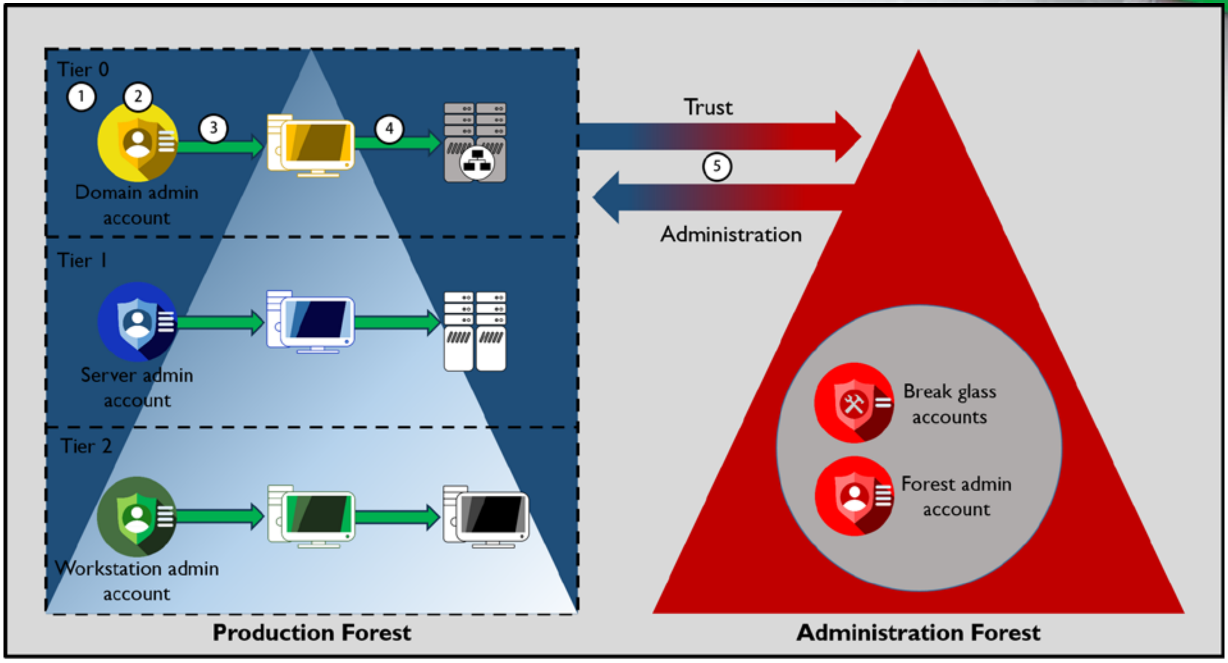

Figure 2: ESAE architecture

*1.) Each privileged account is assigned to a Tier. 2.) The accounts have only those privileges that are required to manage the assigned assets. 3.) Admins must log in to privileged accounts via a dedicated privileged access workstation (PAW) that is dedicated to their own Tier. Admins cannot log in on PAWs dedicated to other Tiers. 4.) Accounts can only manage assets assigned to their Tier. 5.) Accounts for the Production Forest are managed by admins in the Administration Forest.*

**Authentication** is the mechanism that ensures that only authorized users can access accounts. Strong authentication methods, like multi-factor authentication (MFA), assist in defending privileges.[4] Using MFA hinders attackers by requiring them to defeat multiple independent authentication mechanisms. In many cases, MFA systems can be incorporated into existing public key infrastructure or certificate based structures. MFA systems that rely on encryption must be properly configured to avoid known vulnerabilities. This includes migrating to the newest cryptographic algorithms and removing outdated security artifacts such as expired certificates from certificates stores.

Many attacks will circumvent strong authentication mechanisms by leveraging a weak credential recovery process (e.g. when a user forgets their password). Authenticating “in-person” or using a secure out-of-band method for authenticating users assures a strong credential recovery process.

Many other attacks will attempt to bypass strong authentication mechanisms by reusing single-factor authentication assertions (such as Pass the Ticket) or leveraging automated accounts that cannot use multi-factor authentication (such as service accounts). Single-factor authentication assertions are used behind-the-scenes by many services to enable single-sign-on capabilities so users do not need to authenticate over and over. Instead, the user only performs the MFA once and then an assertion that states that MFA has been used is passed to access many services. When an attacker gains access to this single-factor assertion, or, even worse, the master key that signs these assertions, then the attacker no longer needs to satisfy the difficult MFA requirements [5]. Limiting the lifetime of these assertions, periodically re-validating their associated MFA, and protecting assertion signing keys enable an enterprise to realize the full security benefits of strong authentication mechanisms.

Another way to enhance authentication security is with the implementation of a Privilege Access Management (PAM) solution. These solutions provide a centralized management interface for authentication and access control throughout the network. This provides simplified device management and granular least privilege implementation and can often support MFA for otherwise incompatible platforms. In many cases, access controls and management functions can be automated. Most PAM solutions also provide a means to monitor and audit the

[4] For guidance on strong authentication, please refer to *Transition to Multi-factor Authentication,* part of the NSA Cybersecurity Top 10 Mitigations packet.

use of accounts and privileges.

### Monitor for anomalies

Adversaries may succeed in penetrating the network despite all these efforts. The final stage in the defending privileges and accounts lifecycle is to continually monitor for anomalous behavior and changes in the risk posture.[5] Internal and independent auditing measures will help to maintain a consistent perspective of accounts and privileges. Certain security products and operating system features will monitor where and how accounts and credentials are used and even create fake account credential tokens ("honey-tokens") that, when stolen and used, will raise alarms. Develop, maintain, and exercise a plan for responding to anomalies, including plans for how to recover from the most critical account compromises (e.g. golden ticket resets, mass MFA token replacements), which require careful planning [6].[6]

## ARE THOSE PRIVILEGES STILL NEEDED?

The account and privilege defense lifecycle is a continual process designed to adapt to the evolving needs of an organization. Changes in operations, personnel, or devices necessitate changes in accounts and privileges. Regular reviews and monitoring help to protect high value assets by limiting exploitation and insider threat. Strengthening the defense of privileges and accounts is an essential aspect of a defense-in-depth strategy to improve the overall security and resiliency of a network.

## REFERENCES

[1] "Committee on National Security Systems (CNSS) Glossary." CNSSI, 4009-2015, 2015 April 6.

[2] "2018 Data Breach Investigation Report." 11th edition, Verizon, 2018.

[3] "Managing and Controlling Administrative Privileges Explained." ITSB-94, Communications Security Establishment / Centre de la sécurité des télécommunications, 2015 June.

[4] "Active Directory Administrative Tier Model." Microsoft, 2019 June 4. https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/securing-privileged-access-reference-material

[5] "Pass the Ticket". MITRE, 2018. https://attack.mitre.org/techniques/T1097/

[6] "AD Forest Recovery – Resetting the krbtgt password." Microsoft, 2018 August 8. https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/ad-forest-recovery-resetting-the-krbtgt-password

## RELATED NSA CYBERSECURITY GUIDANCE

- "Privileged Access Management," NSA, 2017 April 25. [Online] Available: https://apps.nsa.gov/iaarchive /library/ia-guidance/security-tips/privileged-access-management.cfm
- "Least Privilege," NSA, 2017 April 10. [Online] Available: https://apps.nsa.gov/iaarchive /library/ia-guidance/security-tips/least-privilege.cfm
- "Hardening Authentication," NSA, 2016 November 3. [Online] Available: https://apps.nsa.gov/iaarchive /library/ia-guidance/security-tips/hardening-authentication-update.cfm
- "Hardening Authentication," NSA, 2016 July 21. [Video] Available: https://www.youtube.com/watch?v=fXpKl3Jam-w

### DISCLAIMER OF WARRANTIES AND ENDORSEMENT

The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes.

### CONTACT INFORMATION

Client Requirements and General Cybersecurity Inquiries
Cybersecurity Requirements Center (CRC), 410-854-4200, email: Cybersecurity_Requests@nsa.gov

[5] For more information on threat hunting, please refer to *Continuously Hunt for Network Intrusions*, part of the NSA Cybersecurity Top 10 Mitigations packet.

[6] For more information on system recovery, please refer to *Exercise a System Recovery Plan,* also part of the NSA Cybersecurity Top 10 Mitigations packet.