Internal Network Security Cheat Sheet

Compass Security, Version 1.0, May 2021
https://www.compass-security.com

This Cheat Sheet provides a list of important mitigation steps against common security issues, which are regularly identified during penetration tests of on-premise networks.
More information, including implementation details, can be found in the following guide on GitHub:
https://github.com/CompassSecurity/NWSecurityGuide

Credential Discovery

Unprotected sensitive information, for instance plaintext credentials, can be abused by an attacker. The following points should be considered as mitigation measures:

- Store Credentials Securely
  Store passwords securely such as in password managers. **Do not save them** in GPOs, scripts on SYSVOL shares, files on shares, object descriptions in AD or in the userPassword field in Active Directory.
- Restrict Permissions on Shares
  Restrict share **permissions** to the **minimum required**. Do not use the Built-In groups "Authenticated Users", "Domain users" or "Everyone" to grant permissions.
- Limit SMB Access
  Limit SMB access to any system by using **firewall rules** to only allow **whitelisted** sources.
- Exclusively Use Encrypted Protocols
  Replace plaintext protocols such as telnet, FTP or HTTP with their encrypted counterparts.

Weak Credentials

Humans tend to choose weak passwords by following certain patterns and reuse them across different services. This makes it possible for attackers to guess valid passwords (password spraying attacks & brute-forcing). The following points should be considered as mitigation measures:

- Enforce Strong Password Policy
  Strong passwords use a length of at least **fourteen characters** consisting of **lowercase, uppercase, numbers and special characters**. **Prevent commonly known passwords**, by checking passwords against breached password lists.
- Use Unique Local Admin Credentials
  Change local admin passwords **on a regular basis** and choose **different ones** for every workstation and server. Microsoft **LAPS** can be used to automate this.
- Change Default Credentials
  Change credentials for services and third-party devices upon first usage. **Default values are well known** and can easily be found online to connect to services and perform further attacks.
- Configure Account Lockout
  Enforce **account lockout** for several minutes after **10 or fewer failed login** attempts. Set the **lockout duration** and reset lockout count to 15 minutes or more.
- Enforce Multi-Factor Authentication
  Enforce MFA on all logins supporting it, especially remote access services, security related systems and all internet facing services. Choose **FIDO2** wherever possible and prioritize usage of an **authenticator app** over SMS or e-mail.

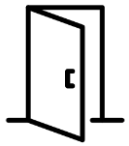
Overprivileged Accounts

Accounts and services are often granted too many privileges, increasing the risk of lateral movement once such an account is compromised. The following points should be considered as mitigation measures:

- Assign Permissions to The Least Privilege Principle
  Separate accounts by tasks, classification, environment, etc. and grant the necessary **permissions** according to the **least privilege principle**.
- Remove Local Administrator Rights
  Remove local admin rights from all users except the built-in Administrator on all workstations. Provide high privileges only temporarily when required.
- Do Not Use Domain Administrators for Daily Tasks
  When logging on to clients and servers in the domain, **never use Domain Administrator** accounts. Also, do not provide service accounts with these high privileges. Use domain admins only when logging on to Domain Controllers.
- Use Group-Based Access Control
  Define AD groups, **assign** the according users and **grant access** to resources for said groups.
- Minimize High Privileged Admin Accounts
  Review AD accounts and **remove** the following **privileges** where not needed: Domain Admins, Enterprise Admins, BUILTIN\Administrators, Schema Admins, Account Operators, Backup Operators, Print Operators, Server Operators.
- Implement Least-Privilege Administrative Model
  Harden administrative accounts. Use built-in local admins for initial build and disaster-recovery only, deny remote logon for built-in local admins and disable them. Apply security controls for built-in admin groups on DCs to allow local and remote logon only for disaster-recovery. Create a management account for protected groups in case temporary admin access is required. Supervise and audit account changes using Privileged Identity/Access Management (PIM/PAM) software, audit and alert changes to the administrative group. Use separate admin accounts for different security classifications and tiers.

COMPASS SECURITY

Missing Network Segmentation and Segregation



A missing or poorly designed firewall concept allows an attacker or malware to spread to other systems and services after getting foothold in the network. The following points should be considered as mitigation measures:

- Implement Network Segmentation
  Systems should be separated into **different network zones based on their sensitivity and data classification**. Create e.g., a DMZ for Internet-facing systems, client zone for user workstations, secure zone for systems with sensitive data, management zone for management interfaces and management systems (e.g., Jump Hosts), zone for PAWs, zone for domain controllers, zone for VoIP systems, etc.
- Whitelist Network Traffic
  Allow only **legitimate network traffic** which is authenticated and authorized, instead of denying unallowed traffic. A "deny any" rule at the end of every ruleset should block any unintended connections.
- Deploy Strictly Configured Host-based Firewalls
  Enable **host-based firewalls** on all systems. **Block traffic** in general and **whitelist** the necessary services on restricted ports and IPs only.
- Secure Wireless Networks
  Configure wireless infrastructure according to **best practices**. Separate guest and enterprise networks, prefer WPA2 Enterprise or less recommended WPA2 PSK with at least 12 characters, use Rogue Access Point detection, isolate clients, protect Access Points from physical access.

Relaying Attacks

By intercepting and manipulating communication in the network, an attacker can abuse the privileges of the compromised connection in relay attacks (e.g., NTLM Relaying) to connect to high-value targets. The following points should be considered as mitigation measures:

- Enforce SMB & LDAP Signing
  Enable and **enforce** SMB and LDAP **signing** on all Windows server and clients.
- Disable NetBIOS and LLMNR
  Disable NetBIOS, LLMNR and Proxy Auto Detection on all clients and servers.
- Disable Spooler Service
  To **prevent exposing the computer account credentials** of a system, disable the spooler service on all DCs (primarily) as well as windows servers not needing printing functionality.

Tools for Identifying Issues

- Privileges of Domain Accounts:
  https://github.com/BloodHoundAD/BloodHound
- Sensitive Data on Shares:
  https://github.com/SnaffCon/Snaffler
- Password Policies
  https://www.pingcastle.com
- Systems and Services in Networks
  https://nmap.org/
- System Hardening
  https://www.cisecurity.org/cis-benchmarks/

Missing Hardening of Systems and Services

Default settings of operating systems, applications and services are often poorly configured and provide an increased attack surface. The following points should be considered as mitigation measures:

- Install EDR or Antivirus
  Install **AV** on all devices. To increase threat detection using behavior analysis and real-time responses an Endpoint Detection and Response (**EDR**) solution should be considered on top of it. **Prevent disabling** of either tool and manage and monitor them centrally.
- Disable or Restrict Macros
  Disable macros in Office products or only allow signed macros to be executed.
- Implement Patch Management Process
  Define and follow a process to **install the latest security updates** on servers, workstations and other devices.
- Enforce BitLocker on Clients
  Encrypt hard disks of all workstations using BitLocker. BitLocker should be used with TPM and at least require a **PIN at startup**.
- Enable Credential Guard
  Prevent credential theft by enabling the credential guard security feature.
- Enable AppLocker
  Use Microsoft Windows Defender Application Control and Microsoft AppLocker to **restrict the allowed programs** for users using a **whitelist** approach.
- Limit Cached Credentials
  Disable caching of domain passwords using GPO.

For more information, please check out our guide on GitHub:

https://github.com/CompassSecurity/OnPremSecurityBestPractices

COMPASS SECURITY