Cybersecurity

Subject: User account security

Ensuring necessary security properties of both front-end and back-end software in the big-data and cloud computing realms requires profound knowledge and hands-on skills in several fundamental topics which include operating system security, authentication and authorization, account management, network access management or end-to-end encryption, among others. To facilitate achieving that goal we invite the student to a set of challenge-based exercises focused on the afore-mentioned topics.

We will start with the operating system security, as it plays an essential role in all fields of the modern IT systems. The first challenge will address user account security issues in the Microsoft Windows operating system.

1. User Accounts

1.1 Accounts

1.1.1 Accounts identifiers

The operating system must uniquely identify each user (this rule applies not only to regular user accounts, but also to user groups, system accounts, and system services). In Windows operating system, each user account has an assigned unique Security IDentifier (SID), which is a 48-bit value composed of several parts. The `user2sid` tool displays the SID of the chosen account, e.g.:

```
C:\> user2sid JamesBond
S-1-5-21-3568558243-2807218454-1792209693-1001
Number of subauthorities is 5
Domain is VIRTUAL-1
Type of SID is SidTypeUser

C:\> user2sid  SherlockHolmes
S-1-5-21-3568558243-2807218454-1792209693-1002
Number of subauthorities is 5
Domain is VIRTUAL-1
Type of SID is SidTypeUser
```

The beginning of each SID: S-1-5, common to all accounts, is called Identifier Authority, and indicates the issuer—Windows operating system (`SECURITY_NT_AUTHORITY`). The 3 central numbers of the user's SID, *Subauthorities*, identify the computer or network domain. The last part, RID (Relative ID), is the system-local identifier of a specific account.

The service SID is built a bit differently, because the Subauthority values depend on the registered service name, not the domain. Service ID can be obtained using the `sc` tool, e.g.:

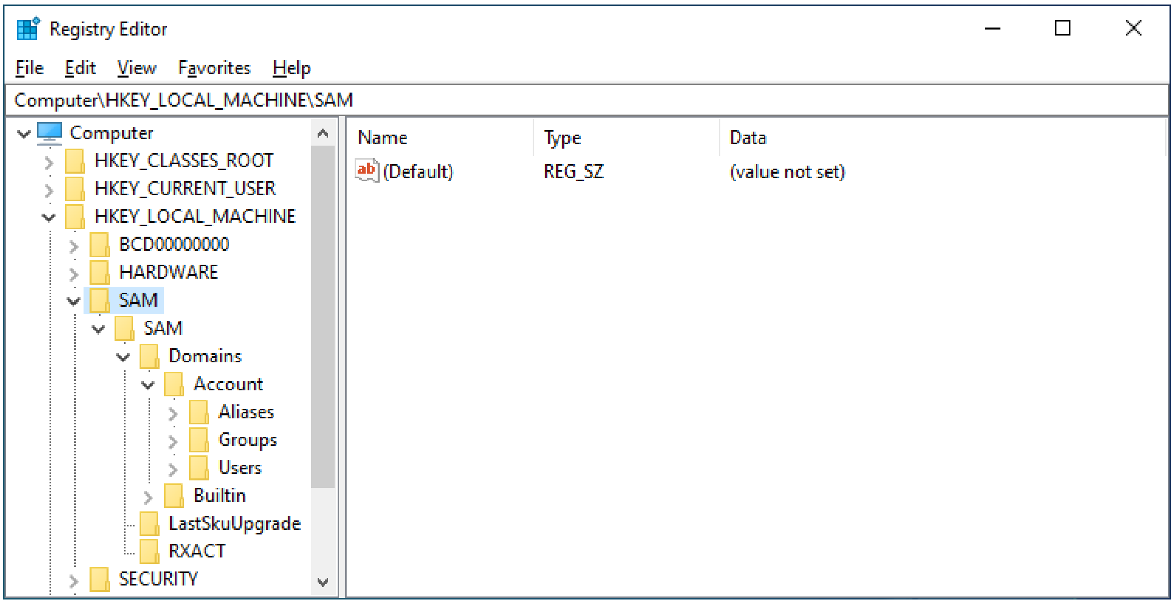
```
C:\> sc showsid dnsclient
NAME: dnsclient
SERVICE SID: S-1-5-80-29309936-11428605-11060112-10997463-2449220572

C:\> sc showsid dhcpclient
NAME: dhcpclient
SERVICE SID: S-1-5-80-31585644-31288558-19997162-40864264-3586357366
```

Full local user accounts information can be retrieved from WMI (Windows Management Instrumentation), e.g. by typing the command:

```
C:\> wmic useraccount list full
```

1.2 Passwords

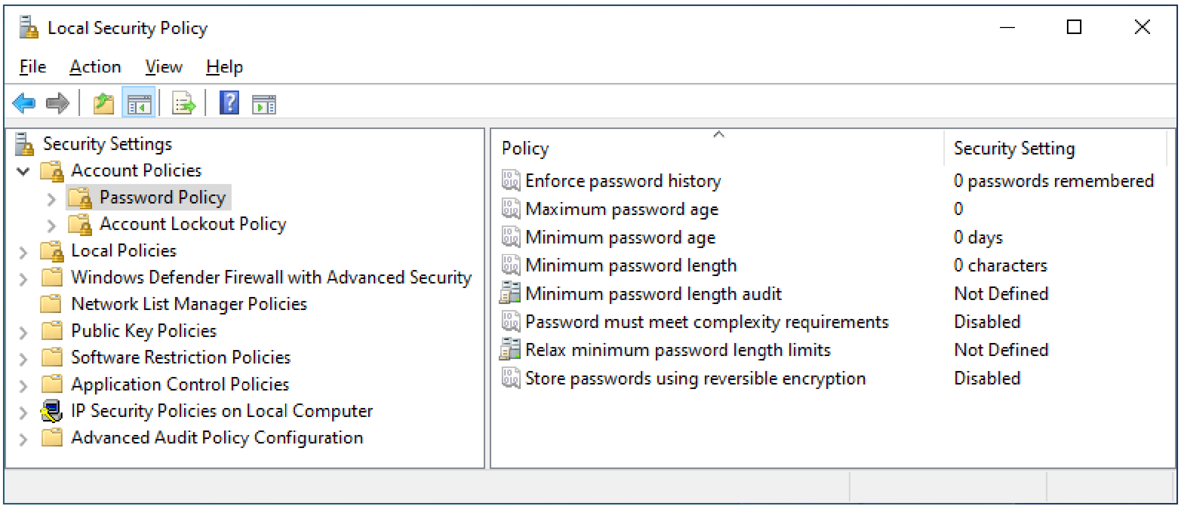
User accounts are locally managed by Security Accounts Manager (SAM). The SAM database, located in the HKLM \ SAM system registry, reserved only for the SYSTEM account, stores, inter alia, account passwords.



Name	Type	Data
ab (Default)	REG_SZ	(value not set)

1.2.1 Strong password policy

User passwords may be subject to certain restrictions, automatically verified by the operating system. Restriction parameters can be accessed via the Local Security Policy program (secpol.msc). This application offers access to parameters grouped in Password Policy and Account Lockout Policy.


Local Security Policy
File Action View Help
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
Windows Defender Firewall with Advanced Security
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Computer
Advanced Audit Policy Configuration

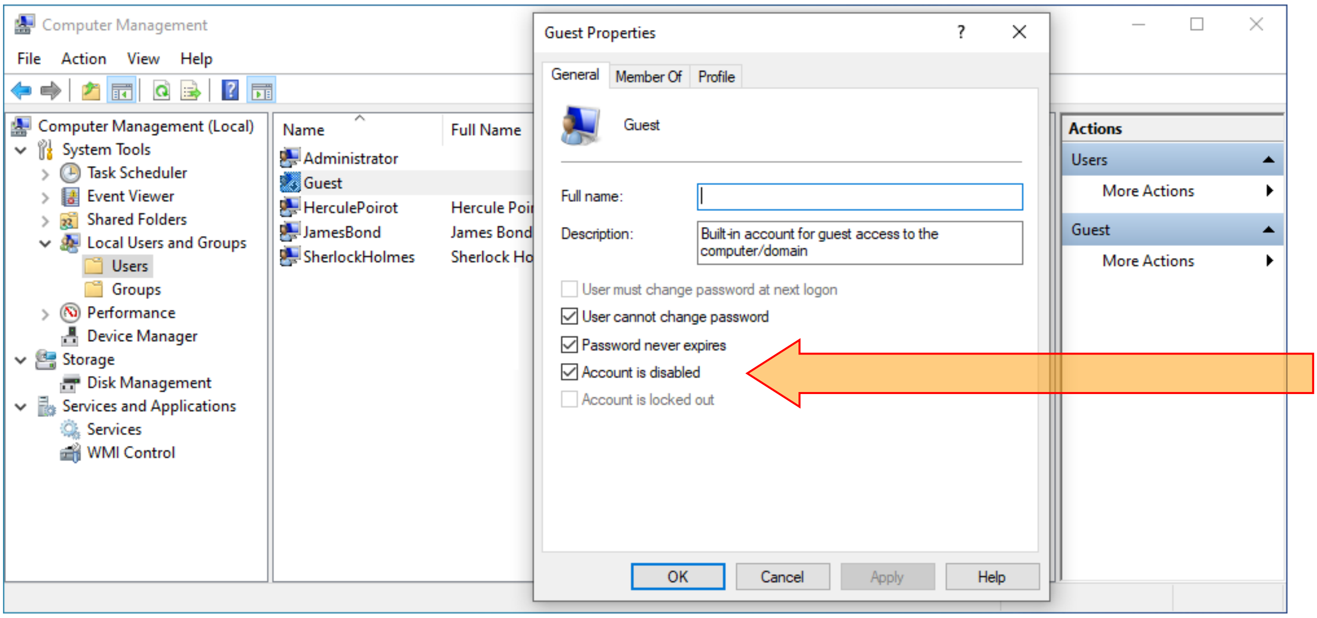
Policy	Security Setting
Enforce password history	0 passwords remembered
Maximum password age	0
Minimum password age	0 days
Minimum password length	0 characters
Minimum password length audit	Not Defined
Password must meet complexity requirements	Disabled
Relax minimum password length limits	Not Defined
Store passwords using reversible encryption	Disabled

1.3 Logging events audit

For obvious reasons, privileged accounts (accounts with administrative privileges) should be carefully protected against unauthorized use. You can enable logging login-related events in Local Security Policy section Local Policies → Audit Policy. Logged events can be viewed using the Event Viewer program (section Windows Logs → Security).

1.4 Account deactivation

In a security conscious environment, all user accounts except the necessary ones (with particular consideration of default accounts set up by the system or other applications), should be disabled (or even removed). You can identify and disable unused accounts using the Computer Management application (compmgmt.msc, also available in the Computer context menu).



Guest

Full name:

Description: Built-in account for guest access to the computer/domain

☐ User must change password at next logon
☑ User cannot change password
☑ Password never expires
☑ Account is disabled
☐ Account is locked out

Comments:

1. Administrator password in the lab installation is: `P@ssw0rd`
2. James Bond account in the lab installation has password: `walther9mm`

Resources:

user2sid (https://www.windowsecurity.com/whitepapers/windows-Enumeration-USER2SID-SID2USER.html)
winfo (https://www.ntsecurity.nu/toolbox/winfo/)

Further reading:

https://technet.microsoft.com/pl-pl/library/cc780850%28v=ws.10%29.aspx
https://technet.microsoft.com/pl-pl/library/cc787567%28v=ws.10%29.aspx
https://www.eventid.net

Problems to discuss:

- What's the difference between the following user groups: Users, Authenticated Users and Everyone?
- Is the failed-login attempt counter (set in the Account Lockout Policy) reset after a successful login?
- When the user's password is required to unlock the computer locked by a screen saver or with the use of ⊞L key, are the incorrect password inputs treated as failed-login attempts?
- Check out the Audit Policy settings. How is auditing "logon events" different from auditing "account logon events"?