Disk Forensics II

1.1 Windows Registry

The Windows Registry is a database that contains the settings of Windows and its applications. It is designed to have a centralized, hierarchical, scalable configuration, have fast access to configuration data, and be employed for system restore and backup. It stores configuration settings and system information, user profiles, application settings and start-up programs, network settings, security policies and so on. It may contain traces related malicious or suspicious activities on the system. It helps analysts identify malware persistence mechanisms and allows obtaining user/program information.

The representation is simplified, keys are represented as folders, which can be organized in sub-keys.

Windows Registry Files. NTUSER.DAT stores user-specific settings, including desktop settings, file associations, and installed software settings. SYSTEM contains information about hardware and system services. SOFTWARE holds software settings for both the system and application. FTK Registry Viewer is best for opening external registry files, because it opens even corrupted ones.

1.2 Windows Credentials

LM Hash were used in early windows versions up to Windows XP, very weak hashing mechanism that can be easily cracked. NTLM was introduced in Windows NT and was used alongside LM Hash in subsequent Windows versions. It uses no truncation, and uses the MD4 hashing mechanism. Since Windows 7, credentials security has improved significantly, thanks to Kerberos and a virtualization-based security (starting from Windows 10). Windows Active Directory is a centralized service that manages networks. Each user is an organizational unit, which are organized in domains. Group of domains are called trees, and trees into forests. Organizational Units are logical containers that organize objects in a domain according to specific criteria. For example, they can represent users or computers. Group Policies are the rules applied to manage such units. Authentication and Authorization is managed through Kerberos.

LSASS is the process that manages authentication in windows. It is a subsystem that defines local security policies and checking users' rights, implemented via the lsass.exe process. HKEY_LOCAL_MACHINE/Policy/Secrets contain special secrets that are related to Active Directory or Data Protection API (DPAPI). The lsadump module of mimikatz allow you to access the secret registry key.

Windows manages logs through event viewer.