4. Microsoft Authentication

Module 8

Password Cracking

- **Security Accounts Manager (SAM) Database**:
  - Windows stores user passwords in SAM, or in the Active Directory database in domain. Passwords are never stored in clear text; passwords are hashed and the results are stored in the SAM.
- **NTLM Authentication**:
  - The NTLM authentication protocol types:
    - NTLM authentication protocol
    - LM authentication protocol
  - These protocols stores user's password in the SAM database using different hashing methods.

Password Cracking

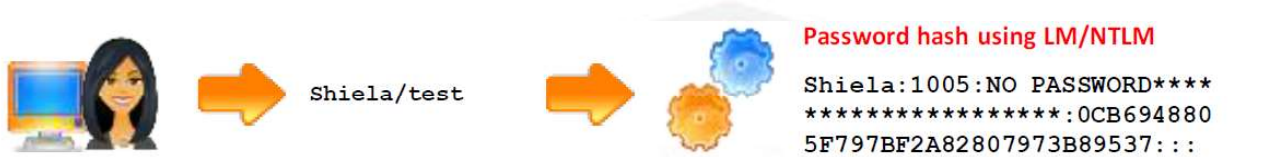
- **Kerberos Authentication**:
  - Microsoft has upgraded its default authentication protocol to Kerberos which provides a stronger authentication for client/server applications than NTLM.

Password Cracking

Security Accounts Manager (SAM)

- It is a database file in Windows XP, Windows Vista, Windows 7, 8.1 and 10 that stores users' passwords. It can be used to authenticate local and remote users.
- Beginning with Windows 2000 SP4, Active Directory authenticates remote users. SAM uses cryptographic measures to prevent unauthenticated users accessing the system.
- The user passwords are stored in a hashed format in a registry hive either as a LM hash or as a NTLM hash. This file can be found in %SystemRoot%/system32/config/SAM and is mounted on HKLM/SAM.

Password Cracking



SAM File is located at `c:\windows\system32\config\SAM`

```
Administrator:500:NO PASSWORD**********************:61880B9EE373475C8148A7108ACB3031:::
Guest:501:NO PASSWORD**********************:NO PASSWORD**********************:::
Admin:1001:NO PASSWORD**********************:BE40C450AB99713DF1EDC5B40C25AD47:::
Martin:1002:NO PASSWORD**********************:BF4A502DA294ACBC175B394A080DEE79:::
Juggyboy:1003:NO PASSWORD**********************:488CDCDD2225312793ED6967B28C1025:::
Jason:1004:NO PASSWORD**********************:2D20D252A479F485CDF5E171D93985BF:::
Shiela:1005:NO PASSWORD**********************:0CB6948805F797BF2A82807973B89537:::
```

User name | User ID | LM Hash | NTLM Hash

Password Cracking

Domain Controller

- A domain controller (DC) is a server that responds to security authentication requests within a Windows Server domain. It is a server on a Microsoft Windows or Windows NT network that is responsible for allowing host access to Windows domain resources.
- A domain controller is the centerpiece of the Windows Active Directory service. It authenticates users, stores user account information and enforces security policy for a Windows domain.
- Beginning with Windows 2000, the primary domain controller and backup domain controller roles were replaced by Active Directory.

Password Cracking

Active Directory

- Active Directory (AD) is a Microsoft product that consists of several services that run on Windows Server to manage permissions and access to networked resources.
- Active Directory stores data as objects. An object is a single element, such as a user, group, application or device, such as a printer.
- AD DS verifies access when a user signs into a device or attempts to connect to a server over a network.
- A forest is formed by a set of multiple and trusted domain trees and forms the uppermost layer of the Active Directory.

Password Cracking

- **Lan Manager (LM) Hash:** It is an encryption mechanism used by Microsoft before it released NTLM. It is a one way hash allowing user to enter their credentials on a workstation and encrypt it. **It is not truly one way.**
- Password was padded to 14 bytes. Each 7 byte half is encrypted with DES with separate keys. This makes it weaker.
- It is susceptible to brute force attacks.
- LM hashes have been disabled in Windows Vista and later Windows operating systems, LM will be blank in those systems.

Password Cracking

New Technology Lan Manager (NTLM) Authentication

- It includes LM version 1 and 2, and NTLM version 1 and 2. It is based on challenge-response mechanism. It proves the server that user knows the password associated with an account.
- A resource server must perform either of the actions to verify the identity of a user:
  - Contact a domain authentication service on domain controller for a computer's domain, if account is a domain account
  - Look up the computer's or user's account in the local database, if the account is a local account.

Password Cracking

- **Core operations of NTLM:**
  - **Authentication:** It provides a challenge-response authentication mechanism.
  - **Signing:** The NTLMSSP applies a digital signature to a message. NTLM deploys a symmetric signature scheme (MAC) which is valid signature that can only be generated with a common shared key.
  - **Sealing:** NTLMSSP uses a symmetric key encryption with provides confidentiality.
- **NOTE:** Microsoft has upgraded its default authentication protocol to Kerberos, which provides strong authentication for client/server applications than NTLM.

Password Cracking