IT SECURITY ACADEN

Authentication, Identification and Authorisation



Authentication is verifying the identity of a user

To authenticate, you have to prove you are who you claim to be IT SECURITY ACADEMY



Identification is stating who you are

It is enough to simply submit your identity



Authorisation is allowing an authenticated user to take some action

Operating systems authorise each operation users take

You can authenticate programs and information as well as users

You can verify the identity of users against:

- Passwords, or information only they should know
- Data only they possess
- Biometrics, or the unique traits of users

 P + 1 + 1 (dimensioner statements) (Terraris Anticipation) (Second Statements - 1 and	
HOW SECURE IS MY PASSWORD?	
•••••	
Command Research in the Suppl 201 March Used Presentering The Typercond V weight commandly and IT. Should be called an advance research The Typercond V weight commandly and IT. Should be days, That, a Hard Andre V The Typercond V and the Typercond V and the Andre V and	
Yearan at a firm Materia New Taward to find distance (allow or News (Yanna) Tay around the first have been first have been for the second statement from Backdown: This on is to extend only propose only. These State	
	- 40



Every authentication method used must protect the identity of users

Mistake number one is using the same identity across multiple different systems

	(* + 1 + 1 +) (disease segments) (Canada Sanadan (* 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1	-
H	OW SECURE IS MY PASSWORD?	
[*****	
103	Common Password: In The Top 529 Mind Used Persenants Visur password is viny contenting used. It invalid he conduct stream materia	
	Phanging The Standard Muniford All residues of the standard and standard standards standards All residues of the standard standard standard standards standards All residues of the standard standard standard standards	
	Bood a better parametel? Try Hise Better Is My Personnel is deter the <u>Histo No.A Commet</u>	
-	ADVERTISABLEST	
-	Venin 10 feet Alana New	
	Towards to and America Soliday Allow we Tolena et Soliday (Towards The mean Honorea Mc Ling), the Soliday Soliday Soliday (Linguist Eggs Backdated): This are to be obtained propose only <u>Soliday Linguist</u>	



Every authentication method used must protect the identity of users

Mistake number one is using the same identity across multiple different systems





The verification of a password does not have to involve checking the submitted string against a password stored on a computer





Windows doesn't store user passwords. It only stores credentials generated from a given password. They can have the following formats:

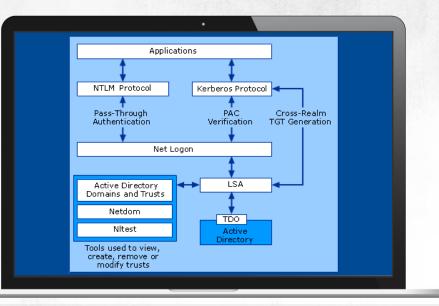
- LM "hash" (the LANMAN hash)
- NT hash (the NT LAN Manager hash, known as the Unicode password)
- Cashed credentials, derivation of NT hashes





The Winlogon process is responsible for authenticating users. One of its components is the msgina.dll library

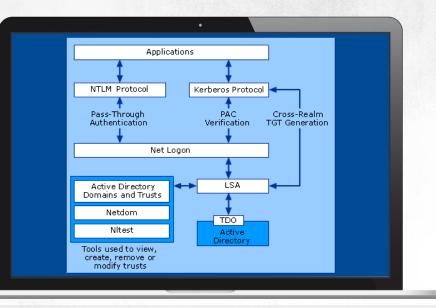
GINA sends submitted data to the LSA subsystem service, and LSA forwards them to a default Security Support Provider (SSP)





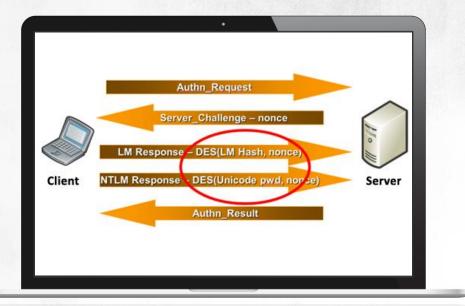
Kerberos is the default SSP in Windows 2000 and newer systems

If Kerberos cannot authenticate a user, user credentials will be sent to the next SSP, NT LAN Manager (NTLM)



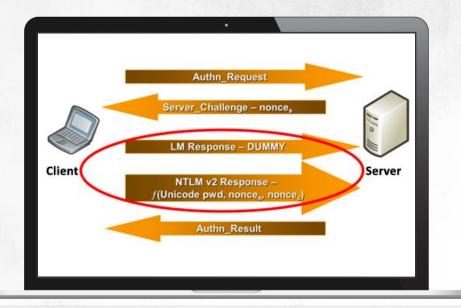


If a local client is to be authenticated, credentials are sent in the MSV1_0 authentication package to the Security Accounts Manager (SAM) file, where they are checked against an encrypted list of passwords





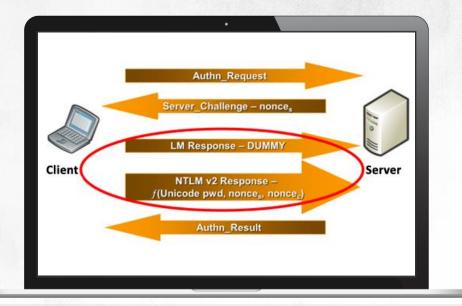
But if the authentication process is to be applied to a remote client, credentials are sent over a network and checked against data saved in a domain controller's or a remote client computer's SAM





In Microsoft Windows networks user identity may be verified using the following protocols:

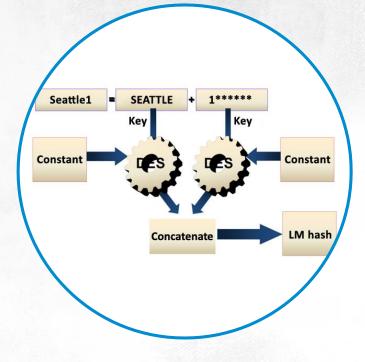
- LM, which should not be used
- NTLM, which also should not be used today
- NTLM v2, which ensures a basic level of security, including the mutual authentication feature. NTLM v2 should be used in workgroups
- Kerberos v5, which is the default authentication protocol in Windows 2000 systems that are members of an AD domain





LM

This protocol makes use of the DES algorithm and a fixed key (constant) to encrypt passwords

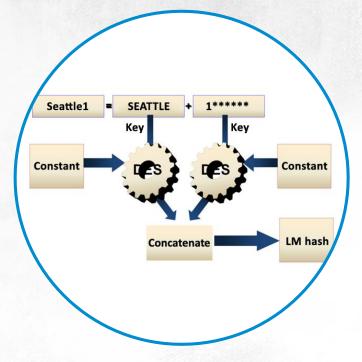




LM

The list of faults is pretty long:

- Passwords are converted to uppercase before encryption
- Only alphanumeric characters are allowed
- Padded with NULL (ASCII 0 code) to 14 characters if a password is shorter. Because LM hashes are deterministic, they do reveal the password's real length (the padding in the passwords always gets the same LM hash characters)
- Split a password into two seven-character halves. Because both parts are DES-encrypted independently and resultant ciphertexts are concatenated, the password parts may be cracked independently. This means that:
 - The LM hash is not 14-character, it has two 7character parts
 - To go over all passwords, a brute-force attack needs to only do about 6.8*10¹² operations



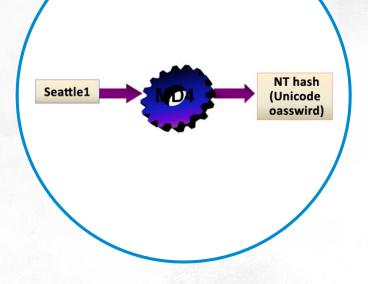


NTLM

NTLM uses a hash function to encrypt passwords NT hashes:

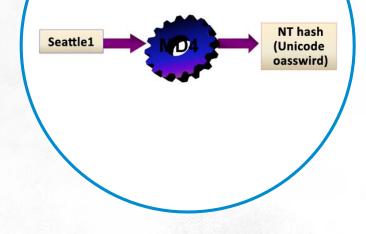
- Are case-sensitive
- Allow passwords to be longer than 14 characters (the maximum length is 127 characters)
- Brute-force attacks need to go over more possibilities to succeed:
 - For passwords that contain the same character set as LM hash there are about 4.6*10²⁵ passwords to check
 - For a 14-character passwords containing any characters there are about 2.7*10⁶⁷ passwords to check
 - For a 127-character password there are about 4.9*10⁶¹¹ passwords to check
- Are also deterministic





NTLM

Windows 2000 and Windows XP systems with default settings store both NT and LM hashes. From Vista onwards the Windows systems only store NT hashes

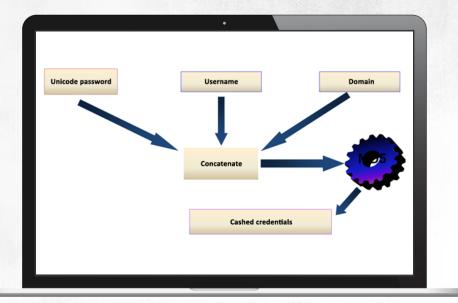




Cashed Credentials

Cashed credentials can be used to allow users to reconnect to remote computers, if the users have been authenticated before

Unlike LM and NT hashes, cashed credentials stored on a local computer are not susceptible to cracking





Cashed Credentials

Even if attackers succeed in reversing a twiceused hash function, it only gives them the ability to log onto a specific remote host, and as thee user whose NT hash was used to calculate the cashed credential

The SAM is also fully encrypted using a Windows startup key

Re sta	assword Startup equires a password to be entered during system art
	onfim:
C	International Store Startup Key on Floppy Disk Requires a floppy disk to be inserted during system start. Store Startup Key Locally Stores a key as part of the operating system, and no interaction is required during system start.



Kerberos

Kerberos V5:

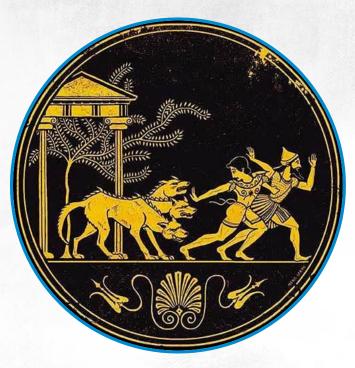
- Is developed on the basis of open standards (RFC 1510 and RFC 1964)
- Enables delegating credentials
- Enables creating cross-realm trust relationships between Windows domains and any Kerberos V5 realms
- Enables creating cross-domain bidirectional, transitive trust relationships
- Doesn't force servers to connect to a domain controller to verify the identity of a client





Kerberos

In AD domains each principal has its own secret: either a longterm key derived from a hash or a private key stored in a certificate issued for the principal







With long-term keys, a shared secret is encrypted by one principal, while another principal decrypts it using the same key

If a user logs on using a smart card, the credential is encrypted using a public key, and decrypted by a KDC with a private key

Every domain controller is a key distribution centre (KDC)

A KDC stores long-term keys as well as grants TGTs and service tickets. Ticket-granting-tickets (TGT) are used to authenticate users, while service tickets are used to enable authenticated users to use a given network service



Kerberos

Every principal (including KDCs) must have the same name: the name is krbtgt

The krbtgt user password is generated automatically and changed on a regular basis

This password is used to calculate the KDC long-term key

This key in turn is used to encrypt TGTs issued by the KDC

Since all KDCs in a domain use the same krbtgt account, all TGT tickets in a domain are encrypted with the same long-term key

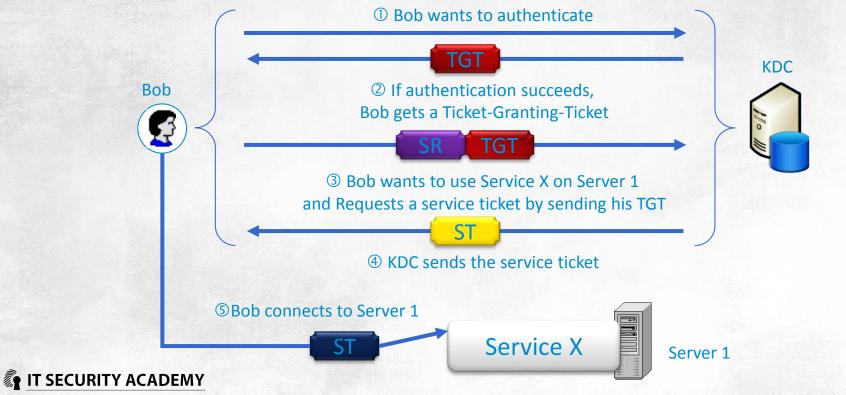
One TGT may be reused multiple times until it expires

TGTs are encrypted with a user's long-term key, and the SIDs they contain are additionally signed by a KDC





User authentication process



Kerberos

Credential Delegation

•
Maria Properties
Member Of Dial-in Environment Sessions
Remote control Terminal Services Profile COM+
General Address Account Profile Telephones Organization
User logon name:
maria @sellers.example.net 💌
User logon name (pre-Windows 2000):
SELLERS\ maria
Logon Hours Log On <u>T</u> o
Account is locked out
Account options:
Smart card is required for interactive logon
Account is sensitive and cannot be delegated
Use DES encryption types for this account Do not require Kerberos preauthentication
Account expires
• Never
C End of: 09 November 2007
OK Cancel Apply



Kerberos

Credential Delegation

Kerberos Tickets	
Class Directed Record LEDG SYMMOLE NET	
Client Principal liz@SELLERS.EXAMPLE.NET	
SELLERS.EXAMPLE.NET - cifs/dc.sellers.example.net - krbtgt/SELLERS.EXAMPLE.NET - krbtgt/SELLERS.EXAMPLE.NET - krbtgt/SELLERS.EXAMPLE.NET - LDAP/dc.sellers.example.net - idap/dc.sellers.example.net	
Service Principal HTTP/app1.sellers.example.net@SELLERS.EXAMPLE.NET Names Times Flags Encryption types Forwardable Forwarded Forwardable Proxy May Postdate Postdated Invalid Initial	T
Renewable HW Authenticated Preauthenticated OK as delegate	
	cifs/dc.sellers.example.net HTTP/app1.sellers.example.net Krbtgt/SELLERS.EXAMPLE.NET LDAP/dc.sellers.example.net Idan/dc.sellers.example.net Idan/dc.sellers.example.net Service Principal HTTP/app1.sellers.example.net@SELLERS.EXAMPLE.NE Names Times Flags Encryption types Proxiable Proxy May Postdate Postdated Invalid Initial Renewable HW Authenticated Preauthenticated OK as delegate



THANKS



