



# Windows Attack - Gain Enterprise Admin Privileges in 5 Minutes

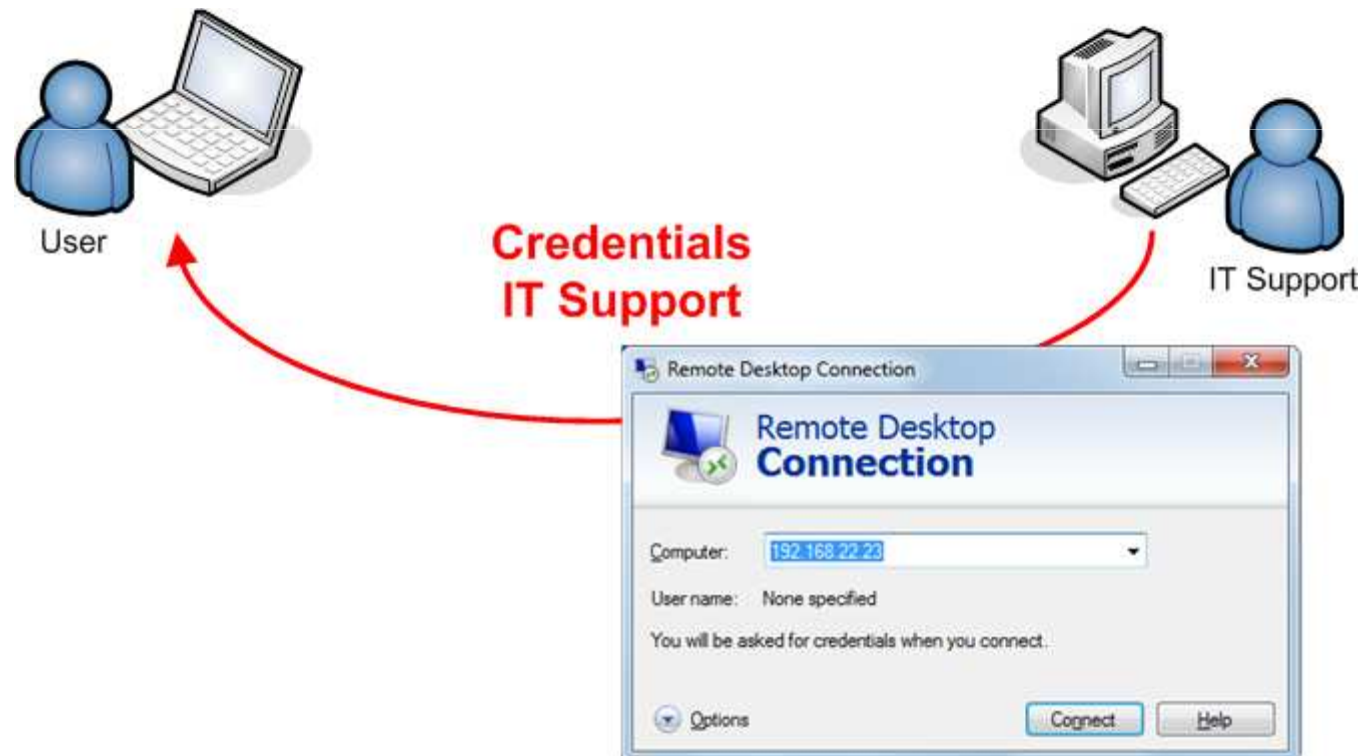
**Compass Security AG,  
Daniel Stirnimann**

Compass Security AG  
Glärnischstrasse 7  
Postfach 1628  
CH-8640 Rapperswil

Tel +41 55-214 41 60  
Fax +41 55-214 41 61  
team@csnc.ch  
www.csnc.ch

## Scenario 1

- ✦ Your employees have a personal computer which has been setup by the internal IT. Support personal can access the computer remotely for administrative access. Can an employee take advantage of this fact and use the login credentials of the IT staff to escalate domain privileges?

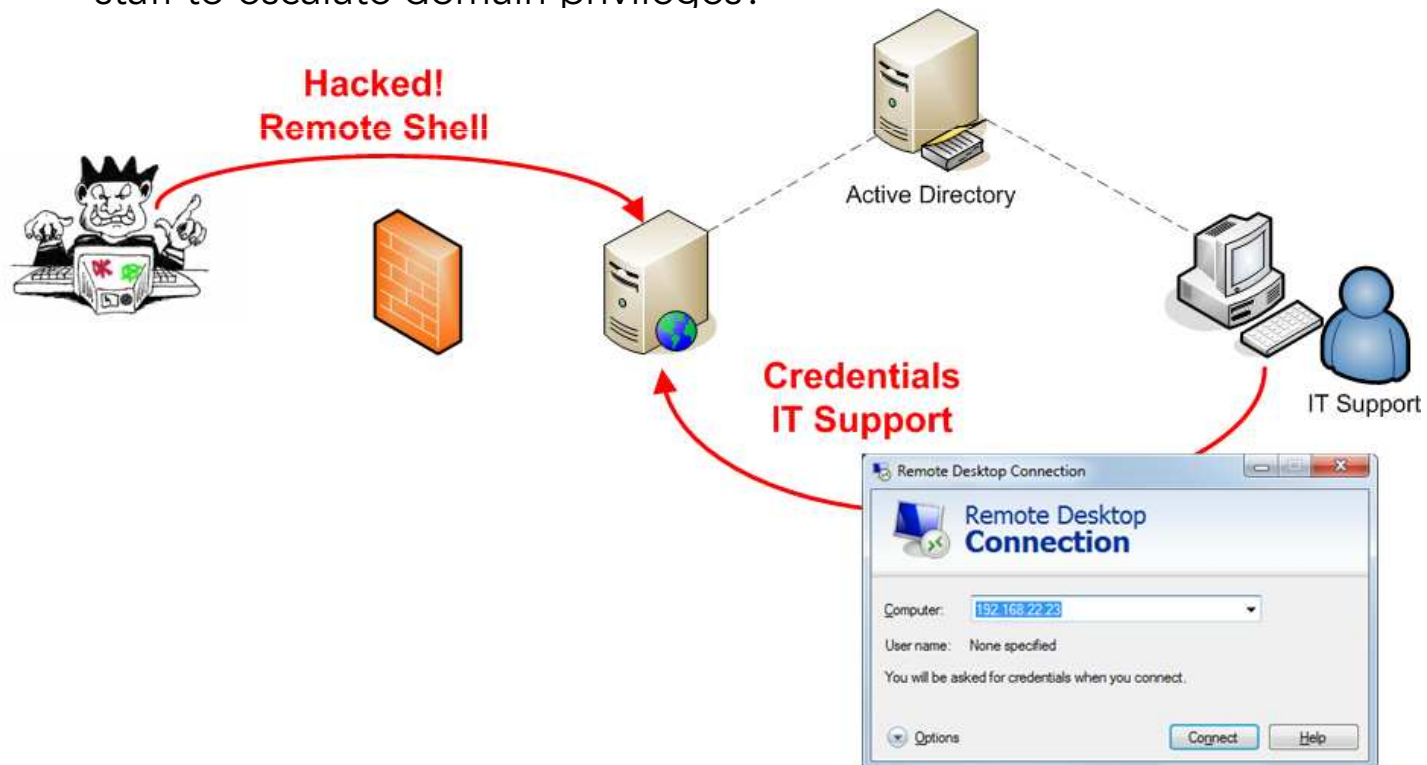


# Introduction



## Scenario 2

- ✦ Your webserver (IIS) is reachable from the Internet. The webserver is joined to the domain and support personal can access the computer remotely for administrative access. Can a remote attacker who has compromised the webserver take advantage of this fact and use the login credentials of the IT staff to escalate domain privileges?



# Introduction



## Goal of this presentation

- ✦ Bring awareness to this topic. It's an old topic but many companies have not taken appropriate measures yet or don't fully understand the security implications.

## Questions I want to answer in this talk

- ✦ Under what circumstances does Microsoft Windows cache credentials?
- ✦ What are the requirements to successfully launch pass-the-hash attacks?
- ✦ How can we protect from this threat?

5 minutes...



Demo

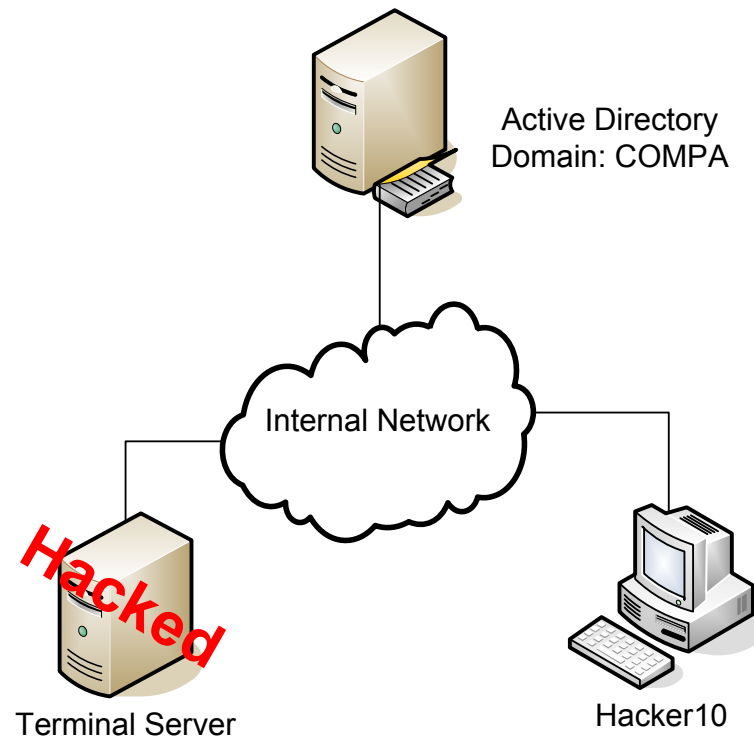


# Topology



## Scenario:

- ◆ Domain Administrator has previously logged in on to the server.
- ◆ Attacker or malicious user has gained root access onto the terminal server and wants to extract cached credentials.



# Agenda

---



- 1. Microsoft Windows Authentication**
- 2. Obtaining the Hash**
- 3. Using The Hash**
- 4. Mitigation Steps**

# Microsoft Windows Authentication



# What is Pass-the-hash?



## What is Pass-the-hash?

- ✦ "Pass-the-hash" allows an attacker to use LM & NTLM hashes to authenticate to a remote host (using NTLM auth) without having to brute-force those hashes to obtain the cleartext password.

## In what scenarios are LM & NTLM hashes used?

- ✦ A computer joined to the Windows Domain will remember the domain credentials so that in offline-mode the user can still logon.

## History

- ✦ First published (theory & exploit code) in 1997 by Paul Ashton (<http://www.securityfocus.com/bid/233/discuss>)
- ✦ Very popular since tool available for the Windows authentication process by Marcus Murray of Truesec (Sweden) during Microsoft TechED 2007

# Windows Authentication History



## Prior Windows NT

- ✦ LM Hash used in the LAN Manager authentication protocol

## Windows NT

- ✦ NTLM Hash used in the NTLMv1 authentication protocol

## Windows NT, SP4

- ✦ NTLM Hash used in the NTLMv2 authentication protocol

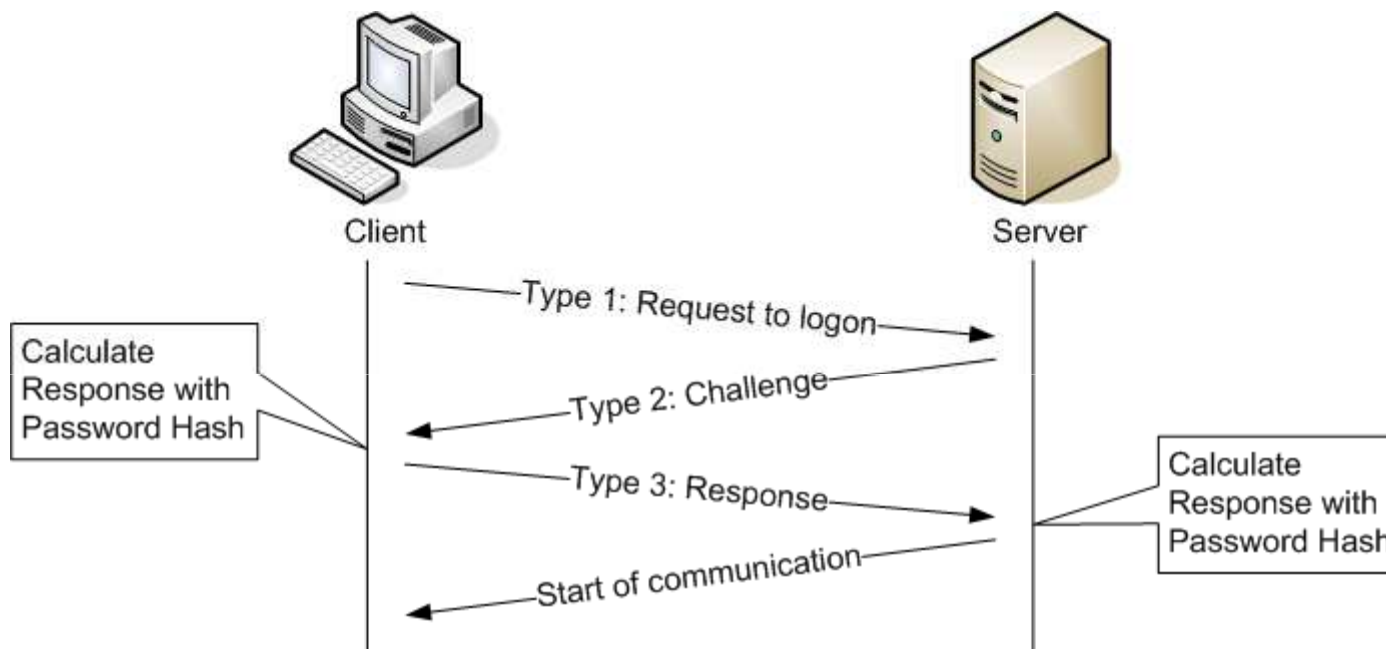
## Windows 2000

- ✦ Kerberos authentication protocol is used by default

## Windows 7, Windows Server 2008 R2

- ✦ NTLM authentication protocol can be disabled completely
  - ✦ Default: LM & NTLMv1 disabled, NTLMv2 enabled
- ✦ Pure Kerberos environment can be setup

## Challenge Response Protocol



- ◆ Response differs depending on authentication protocol version used
- ◆ No LM, NTLM hashes are sent over the wire.
- ◆ Having LM/NTLM Hashes allows to calculate response
- ◆ LM/NTLM Hashes = cleartext password

## Kerberos (default since Win2000)

- ✦ Kerberos systems pass cryptographic key-protected authentication „tickets“ between participating services.
- ✦ User's password (NTLM hash) is converted to a pre-authentication encrypted key that is stored in the workstation's credential cache and can be used by whatever authentication provider is indicated for the logon type.

## Kerberos does not solve the problem completely.

- ✦ Currently no tools support Pass-The-Hash attack for Kerberos
- ✦ In either case, attack shifts to Kerberos...
  - ✦ See Compass Event 2007 - Kerberos Attacks (Röthlisberger, 2007)
  - ✦ See Taming the beast: Assess Kerberos-protected networks (Bouillon ,2009)

# Obtaining the Hash

## Obtaining the Hash



**Obtaining a hash requires local administrator privileges**

**Which hashes (LM, NTLM) are exposed depends on the configuration.**

# Hash exposed in different Scenarios



## Interactive

- ✦ Logon to a local computer to which you have direct physical access.
  - ✦ at the physical workstation
  - ✦ via Terminal Services, via Remote Desktop
  - ✦ run as..

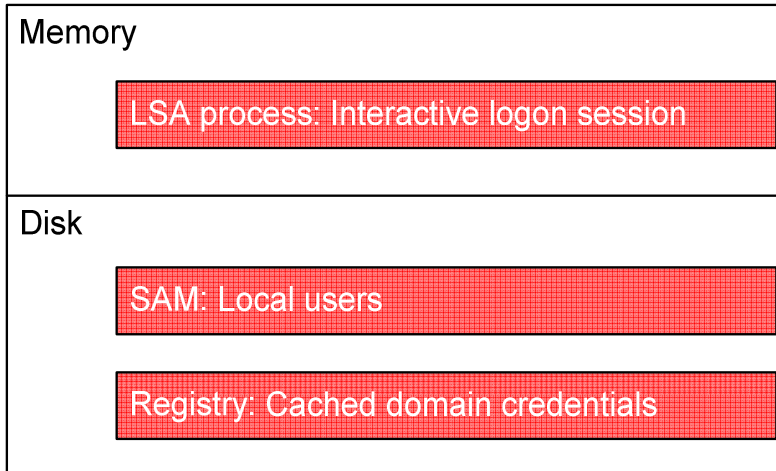
## Network

- ✦ During network logon, the process does not use the logon dialog boxes, such as the Log On to Windows dialog box, to collect data. Instead, previously established credentials or another method to collect credentials is used.
  - ✦ Net Use, Explorer, Net View

# Obtaining the Hash



## Operating System



## Memory

- ✦ During process running time (e.g. runas command, VNC session)

## Disk

- ✦ Hash available throughout a reboot of the operating system
- ✦ Cleaning or preventing the hash from being stored requires a more restrict OS hardening

# Obtaining the Hash



## Memory

- ✦ Dump Hashes stored in memory for active sessions
  - ✦ Pass-The-Hash-Toolkit (whosthere)
  - ✦ Gsecdump
  - ✦ Pwdump7
  - ✦ msvctl

## Disk

- ✦ Dump SAM database
  - ✦ Cain & Abel, pwdump1/2/3/4
- ✦ Registry: Cached Domain Credentials
  - ✦ These cached passwords are stored as hashes in the local systems registry at the values  
HKEY\_LOCAL\_MACHINE\SECURITY\CACHE\NL\$1 through NL\$10
  - ✦ The stored value is the password hash crypted with the username
    - ✦ Limited support by Dump Hash tools

### 1. Accounts that are on the system (initial set-up)

- ✦ Password hash is stored in the registry for the last 10 domain logons

### 2. User B who uses workstation of user A (physical access)

- ✦ Password hash is stored in the registry for the last 10 domain logons
- ✦ Password hash is stored in memory during session time

### 3. User B who uses terminal service on server

- ✦ Password hash is stored in the registry for the last 10 domain logons
- ✦ Password hash is stored on the terminal server during session time. Same applies to Remote Desktop on a workstation.

### 4. User B who uses VNC to remote access workstation and session of user A

- ✦ Password hash is stored on the workstation during session time.

### 5. Credentials provided for "run as..."

- ✦ Hash is stored in memory on the local system as long as the "run as..." process is running.

### 6. Credentials provided for mounting a share

- ✦ Mounting a network share results in a network authentication.
- ✦ The hashes do not appear in the memory of the LSA process. Not an interactive logon.

# Obtaining the Hash



## Other Scenarios?

- ✦ Credentials in the context of automatic software distribution
- ✦ Credentials in the context of full hard disk encryption

## What about PKI/Smartcards?

- ✦ The fact that passwords will be changed into long randomized passwords when you implement smartcard doesn't change anything. The hash is still there and we are simply using that hash, not the password.

### Note:

- ✦ *The security settings in Windows can't force smart-card-based logon for network access, only interactive.*
- ✦ *LM/NTLM can still be used for network logon event if the users are using smartcards to authenticate*

# Using the Hash

## Brute-Force, Dictionary-Attack

- ✦ Gain the plain text passwords and authenticate against other services with the revealed credentials.
- ✦ Feasibility on this attack depends on the exposed Hash and the strength of the password. Typically, LM hashes are cracked within a few hours and NTLM hashes within a few days or weeks.

## Rainbow-Table Attack

- ✦ Also known as pre-computed hash attack.
- ✦ Pre-generated hashes of a password are stored in a file and can be looked up within seconds.
- ✦ The RainbowCrack Project (<http://project-rainbowcrack.com/>) provides a tool to pre-compute rainbow-tables for the following hash algorithm: LM, NTLM, MD5, SHA1, MYSQLSHA1, HALFLMCHALL, NTLMCHALL, ORACLE-SYSTEM, MD5-HALF

## Pass-The-Hash Attack

### Tools

- ✦ Pass the Hash Toolkit v.1.4 (whosthere.exe, iam.exe)  
Hash dumper (local SAM and memory)  
Changes users cached NTLM credentials, so that any Windows tool can use the cached identity.
- ✦ msvctl from Truesec  
Hash dumper (local SAM and memory) and runas like tool with Hash support
- ✦ gsecdump from Truesec  
Hash dumper (local SAM and memory)
- ✦ Pwdump7  
Hash dumper (local SAM)
- ✦ Metasploit
- ✦ Nessus

# Anti-Virus Detection



## Anti-Virus Detection Rate by [www.virustotal.com](http://www.virustotal.com)

Tool	Detection Rate	Submission Date
Test hash usage tool: <b>iam.exe</b> (Pass the Hash Toolkit v.1.4)	27/42 (64.3%)	16.07.2010
Test hash dump tool: <b>whosthere.exe</b> (Pass the Hash Toolkit v.1.4)	17/42 (40.5%)	16.07.2010
Test hash dump and hash usage tool: <b>msvctl.exe</b> (v0.3 from Truesec)	33/40 (82.50%)	26.05.2010
Test hash dump tool: <b>gsecdump.exe</b> (v0.6 from Truesec)	38/42 (90.5%)	27.07.2010
Test hash dump tool: <b>pwdump7.exe</b>	27/41 (65.9%)	25.07.2010

A vertical decorative bar on the left side of the slide. It consists of a solid orange square at the top, followed by a light blue background with a blurred image of a computer keyboard. A white padlock is positioned over the keyboard keys.

# Mitigation Steps

## Least-privilege security principle

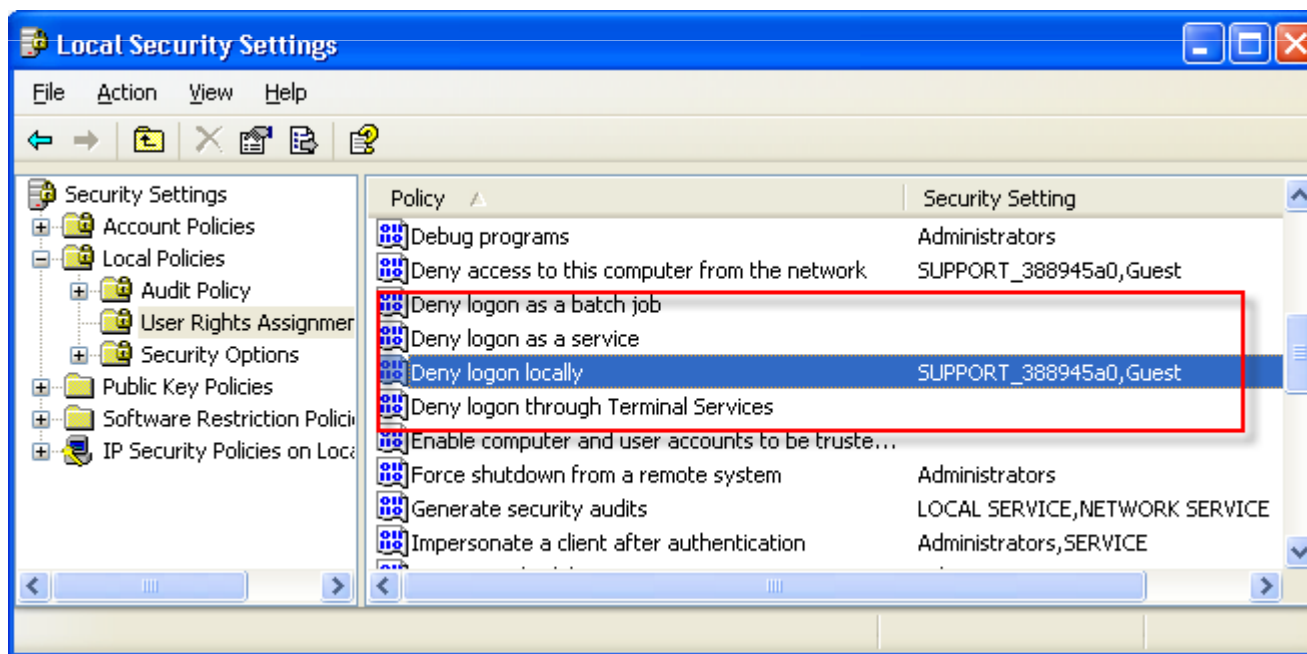
- ✦ Do not give regular employees local administrator rights on their computers. This drastically reduces the number of users that can steal other users password hashes.
- ✦ Only use your domain administrator credentials to logon to domain controllers. Do never logon on to member servers especially terminal servers or workstations with your domain administrator credentials.
- ✦ Domain administrators should have a separate delegated administrator account that they use to logon to member servers and workstations that does not have domain administrator rights.
- ✦ Limit the use of service accounts that have domain administrator rights.

# Least-privilege security principle



## Least-privilege security principle can also be enforced

- ✦ Deny access to this computer from the network
- ✦ Deny logon as a batch job
- ✦ Deny logon as a service
- ✦ Deny logon locally
- ✦ Deny logon through Terminal Service



# Mitigation



## Monitoring

### Privilege Use (System Log)

- ✦ Look for all audit events with the identification (ID) 552

A user successfully logged on to a computer using explicit credentials while already logged on as a different user.

- ✦ Configure high priority alerts on this event ID and immediately review if this event occurs. Some legit service accounts may trigger this ID, so filtering may be necessary.

### Anti-Virus Process

- ✦ The tested tools to dump the hashes (e.g. gsecdump.exe) or impersonate as another user (e.g. iam.exe) are identified by well known Anti Virus products such as Symantec. So, disabled or uninstalled Anti-Virus products should cause an alert as well.

# Mitigation



## Education

### Checklist

- ✦ Support and administrative personnel should be informed about the danger of certain access and authentication methods. A list of DOs and DON'Ts should be created. Examples:
  - ✦ Do NOT login with Domain Admin Privileges on none Domain Controller
  - ✦ Do require the user to login on his workstation after you completed IT support with your account
  - ✦ Do change your accounts password in case you don't fully trust the workstation you have accessed
  - ✦ Etc.

## Protect your password hash

### Patch-Management

- ✦ Keep all computers up to date with the latest operating system and application patches. A user that is not typically an administrator may use a known exploit in the OS or application to elevate their rights to local admin and thus get access to the cached hashes.

### Hardening

- ✦ Restrict GPO settings to limit the exposure of LM and NTLM hashes by disabling LM, NTLMv1 or even NTLMv2 authentication protocols (pure Kerberos environment).

# Protect your password hash



## Cached Domain Logons

- ✦ By default, NT caches the logon credentials for the past 10 users who logged on interactively (CachedLogonsCount)
- ✦ Consider to reduce this setting to 1 logon only.
  - ✦ **Interactive Logon: Number of previous logons to cache: 1 Logon**
- ✦ Note: This requires that after a high privileged user has logged on to a computer, he demands that the "normal" users must logon first to make sure his password hash is not cached anymore

# Protect your password hash



## Local SAM Credentials

- ✦ This setting defines that local SAM credentials are stored as LM hashes as well. For example, the local administrator account's hash is stored as an LM and NTLM hash.
- ✦ Replace outdated Windows systems ( Windows 95, 98 or NT 4) and define the following settings:
  - ✦ **Network Security: Do not store LAN Manager hash value on next password change: Enabled**

# Protect your password hash



## Active LSA Session Credentials

- ✦ If a user is authenticating on the system, the password hashes of this user are stored in memory. The hashes remain in the memory as long as the LSA session is active.
- ✦ Even with Kerberos the NTLM hash of the password is stored. However,
- ✦ Replace outdated windows systems ( Windows 95, 98 or NT 4) and define the following settings:
  - ✦ **Network Security: LAN Manager authentication level: Send NTLMv2 response only. Refuse LM**
- ✦ Best Setting (no Windows 2000 dependencies):
  - ✦ **Network Security: LAN Manager authentication level: Send NTLMv2 response only. Refuse LM & NTLM**
- ✦ Outlook to Windows 7, Windows 2008 R2. NTLM can be disabled altogether in these environments. See settings of Network Security: Restrict NTLM.

### What about other scenarios?

- ✦ Client staging process during network boot (PXE) operates with an install user which has domain administrative privileges. Attacker steals username and password of domain user from the scripts.
- ✦ Using tools such as lsrunase/superscript to run a process with higher privileges in scripts. User credentials provided in an encrypted form but encrypted credentials may be used insecurely.  
<http://www.csnc.ch/misc/files/advisories/CVE-2007-6340.txt>
- ✦ Insecure netlogon-scripts
- ✦ Shatter Attack, Design flaw in the Windows API which is abused to run shell code with the privileges of the target process (VPN-Client, Anti-Virus, VNC)  
[http://www.csnc.ch/misc/files/publications/ShatterAttack\\_CSNC.pdf](http://www.csnc.ch/misc/files/publications/ShatterAttack_CSNC.pdf)
- ✦ Man-In-The-Middle Attacks (ARP Spoofing, Network Traffic Sniffing)

# Questions?



## References



- ✦ Ivan Bütler, Compass Security AG (2007)  
Windows Security – Hash Injection Attacks  
[http://www.csnc.ch/misc/files/publications/Hash\\_Injection\\_Attack\\_E.pdf](http://www.csnc.ch/misc/files/publications/Hash_Injection_Attack_E.pdf)
- ✦ Daniel Röthlisberger, Compass Security AG (2007)  
Kerberos Attacks  
[http://www.csnc.ch/misc/files/publications/2007\\_kerberos\\_v1.0\\_print.pdf](http://www.csnc.ch/misc/files/publications/2007_kerberos_v1.0_print.pdf)
- ✦ Emmanuel Bouillon (2009)  
Taming the beast: Assess Kerberos-protected networks
- ✦ Johansson, J. (2009)  
Windows Server 2008 Security  
Rockland: Syngress Publishing Inc.
- ✦ Christopher Hummel (November 3, 2009)  
Why Crack When You Can Pass the Hash?  
[http://www.sans.org/reading\\_room/whitepapers/testing/crack-pass-hash\\_33219](http://www.sans.org/reading_room/whitepapers/testing/crack-pass-hash_33219)
- ✦ Bashar Ewaida (February 23, 2010)  
Pass-the-hash attacks: Tools and Mitigation  
[http://www.sans.org/reading\\_room/whitepapers/testing/pass-the-hash-attacks-tools-mitigation\\_33283](http://www.sans.org/reading_room/whitepapers/testing/pass-the-hash-attacks-tools-mitigation_33283)

## References



- ✦ Hernán Ochoa (2000). Modifying Windows NT Logon Credential  
<http://www.coresecurity.com/content/modifying-windows-nt-logon-credential>
- ✦ Microsoft TechNet (November 03, 2005). Understanding Logon and Authentication  
<http://technet.microsoft.com/en-us/library/bb457114.aspx>
- ✦ Microsoft TechNet (January 22, 2009). How Interactive Logon Works  
<http://technet.microsoft.com/en-us/library/cc780332%28WS.10%29.aspx>