



O-ISC '07
Ohio Information Security Conference

Password Insecurities and Auditing

Nathan Power

Cox Ohio Publishing

- Windows Local Passwords
- VNC Server Local Passwords
- Password Policy and Procedures

Why Local Passwords?

■ Administrators

- Audit employee passwords
 - Following Policy
 - Not using default passwords

■ Malicious Users

- Escalate privileges on the local host
- Use local passwords to gain access to other systems on the network

■ Just for fun!



Windows Local Passwords

Auditing SAM Passwords



- SAM stands for Security Account Manager
- The SAM file is where accounts local passwords are stored on NT based systems
- SAM file can be found at
C:\WINDOWS\SYSTEM32\CONFIG\SAM

Two types of SAM Hashes

■ LAN Manager (LM)

- First seen in Windows 3.1
- Uses DES hashing algorithm
- Considered weak and insecure
- Enabled by default in Windows 3.1, NT4.0, 98, ME, 2000, XP, and 2003 server

SAM Hashing Example



■ LM Weak DES Implementation

password

PASSWORD

PASSWOR D\0\0\0\0\0\0

40870AE14B6D3BAAD3B435B51404EE EC7100B8D2EDC1D6E6BA18DD62B97B

40870AE14B6D3BAAD3B435B51404EE:EC7100B8D2EDC1D6E6BA18DD62B97B

Two types of SAM Hashes

■ NT Manager (NTLM)

- First seen in NT4.0 service pack 4
- Uses MD4 hashing algorithm
- Considered to be stronger than LM
- Enabled by default in Windows Vista



Audit Methods



- Act of finding plain text passwords by reversing the hash method it's stored with
- This is done by *fast* mathematical means or by *slow* brute force methods

- Time-memory trade off technique
- Hash character sets pre-generated file
- Pre-generated hashes are loaded into memory and compare to stored hashes
- Quicker then generating each hash on the fly

Rainbow Table Character Set

LM 7 Character Set	Table Size	Crack Time
A-Z	610MB	24s
A-Z+0-9	3GB	39s
All Keyboard Characters	64GB	28min

Word List Brute Force

- Take a list of words
- Hash them using the same algorithm
- Compare them to the stored hashes
- Password is found when the hashes match

Word List Brute Force



Word

Hash

golf

757482FBBAC80092318847FEAA321D31F111

388846F7EA8FB117EEDA6C7850B38D6BD06

ocean

A67299EBD2383FFB7823138CBD8802001248

388846F7EA8FB117EEDA6C7850B38D6BD06

password

388846F7EA8FB117EEDA6C7850B38D6BD06

388846F7EA8FB117EEDA6C7850B38D6BD06

MATCH FOUND!

Free Tools to Audit SAM

■ PWDumpX

- Uses DLL injection to dump SAM file
- Can be used via remote

■ Ophcrack

- Uses rainbow tables
- Run from LiveCD

■ John the Ripper

- Multi-platform cracker
- Users word lists and character combinations



SAM Audit DEMO

SAM Cracking Prevention

- Choose strong passwords
 - Alpha-numeric-symbol
 - Extended ascii characters via Alt+num-pad method

- Turn off LM hash storage
 - Group policy, the registry

**HLM\SYSTEM\CurrentControlSet\Control\Lsa\
NoLMHash**

Active Directory Cached Passwords



- Network reliability on Windows 2000 / XP
- Cache last 10 users by default
- Uses MD4 hash



- Cached password hashes stored in registry

HKLM\SECURITY\CACHE\NL\$1 through **\$10**

- Disable caching of credentials

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CachedLogonsCount 0



VNC Server Local Passwords

VNC Server Background



- Remote control another computers GUI
- More diverse then Windows Remote Desktop
- Runs on Windows, UNIX, Linux, and OSX
- Most popular 'RealVNC' & 'TightVNC'

- Only allows 8 character long passwords
- Encrypted password found in registry

RealVNC

HCU\Software\RealVNC\WinVNC4>Password

TightVNC

HCU\Software\ORL\WinVNC3>Password

- DES encrypted password with known key

23 87 107 6 35 78 88 7



VNC Audit DEMO

- Don't use VNC

- Better customer service?

- Use UltraVNC Server

- Allows Windows local or domain authentication



Password Policy and Procedures

Password Policy Example

- Overview
- Purpose
- Scope
- Guidelines

Password Policy Example

■ Guidelines

- Password construction
- Do not reuse passwords
- Do not share passwords
- Change passwords at least every 90 days
- Do not write down or store passwords

- Creating a strong password

Nate lives for Security day in and day out

Nl4sdiado

!¼Nl4sdiado¼!



Questions & Answers