Pass-the-Hash Attacks

Michael Grafnetter
www.dsinternals.com
Agenda

- PtH Attack Anatomy
- Mitigation
  - Proactive
  - Reactive
- Windows 10
PtH Attack Premises

Single Sign-On + Symmetric Cryptography = PtH
PtH Attack Anatomy

Theft → Use → Compromise
PtH Attack Anatomy
Stealing the Hash
Credentials Lifecycle / Attack Vectors
# Hashes in Windows

<table>
<thead>
<tr>
<th>Authentication Method</th>
<th>Hash Function</th>
<th>Salted</th>
</tr>
</thead>
<tbody>
<tr>
<td>LM</td>
<td>DES</td>
<td>NO</td>
</tr>
<tr>
<td>NTLM, NTLMv2</td>
<td>MD4</td>
<td>NO</td>
</tr>
<tr>
<td>Kerberos (RC4)</td>
<td>MD4</td>
<td>NO</td>
</tr>
<tr>
<td>Kerberos (AES)</td>
<td>PBKDF2</td>
<td>YES</td>
</tr>
<tr>
<td>Digest</td>
<td>MD5</td>
<td>YES</td>
</tr>
</tbody>
</table>
Credentials Lifecycle / Attack Vectors

External storage → Sign-on → Use/Cache on client → In transit on network → Authoritative store
Active Directory Database - Offline

- **Files**
  - C:\Windows\NTDS\ntds.dit
  - C:\Windows\System32\config\SYSTEM

- **Acquire**
  - Locally – ntdsutil IFM
  - Remotely – WMI (Win32_Process), psexec
  - VHDs, VMDKs, Backups

- **Extract**
  - libesedb+ntdsxtract
  - Windows Password Recovery
NTDSXtract

esedbexport ntds.dit
python dsusers.py ntds.dit.export/datatable.4
--name Administrator --syshive SYSTEM
-- supplcreds --passwordhashes

Password hashes:
Administrator:$NT$cc36cf7a8514893efccd332446158b1a:::

Supplemental credentials:
Kerberos newer keys
salt: ADATUM.COMAdministrator
Credentials
18 b7268361386090314acce8d9367e55f55865e7ef8e670fbe4262d6c94098a9e9
17 8451bb37aa6d7ce3d2a5c2d24d317af3
3 f8fd987fa7153185
Windows Password Recovery - AD

- Import Wizard
- Import from registry or Active Directory files
  - SAM: C:windows\system32\config\SAM
  - SYSTEM: C:windows\system32\config\SYSTEM
- Import domain accounts (from Active Directory ntds.dit file)
  - NTDSDIT: C:windows\ntds\ntds.dit
  - SYSTEM: C:windows\system32\config\SYSTEM
- Load hash of machine accounts
- Scan system hash for plantest passwords
- Process deleted and hidden accounts, if any

Windows Password Recovery - Empty project

- User name: Administrator
  - Password history hash: Password history hash
  - Description: Built-in account for administering the system
- User name: Guest
  - Password history hash: Password history hash
  - Built-in account for guest access to the system

- User name: Loc-Dc1
  - Password history hash: Key Distribution Center Service Account

- User name: Hizern
  - Password history hash: Password history hash

- User name: Budmunder
  - Password history hash: Password history hash

- User name: Modj
  - Password history hash: Password history hash

- User name: Cigdem
  - Password history hash: Password history hash

- Log window
KRBTGT Account
DEMO

IFM + Windows Password Recovery
Proactive Measures

- Encryption
- RODC
- Backup protection
- Regular password changes
Active Directory Database - Online

- MS-DRSR/RPC
Proactive Measures

- Avoid using administrative accounts
- Do not run untrusted SW
SAM Database

- Offline
  - Files
    - C:\Windows\System32\config\SAM
    - C:\Windows\System32\config\SYSTEM
  - Tools
    - Windows Password Recovery

- Online
  - Mimikatz
DEMO

SAM dump using Mimikatz
Proactive Measures

- Restrict administrative access
- Bitlocker
- Randomize local Administrator passwords
GP Local Admin Pwd Management Solution

Password Settings

- Not Configured
- Enabled
- Disabled

Comment:

Supported on: At least Microsoft Windows XP Professional or Windows Server 2003 family

Options:

Password Complexity:
- Large letters + small letters + numbers + specials

Password Length: 12

Password Age (Days): 30

Help:

Configures AdmPwd password parameters:
- Password complexity: which characters are used when generating a new password
- Default: Large letters + small letters + numbers + special characters
- Password length:
  - Minimum: 12 characters
  - Maximum: 64 characters
  - Default: 12 characters
- Password age in days:
  - Minimum: 1 day
  - Maximum: 365 days
  - Default: 30 days
Credentials Lifecycle / Attack Vectors
Windows Integrated Authentication

Application
  RPC

.NET Application
  .NET Framework

Internet Explorer

SSPI

Kerberos
NTLM
Digest
Schannel
Negotiate
Other

Application Layer
SSPI Layer
SSP Layer
# SSP Cached Creds (SSO)

<table>
<thead>
<tr>
<th>Kerb</th>
<th>Hashes</th>
<th>Plaintext-Equivalent Passwords</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>TGT</td>
<td>LM</td>
</tr>
</tbody>
</table>

### Windows 8.0 and previous
- **Microsoft Account**
  - Kerb: Yes
  - Hashes: Yes
  - Plaintext-Equivalent Passwords: No

- **Local Account**
  - Kerb: Yes
  - Hashes: Yes
  - Plaintext-Equivalent Passwords: No

- **Domain Account**
  - Kerb: Yes
  - Hashes: Yes
  - Plaintext-Equivalent Passwords: No

### Windows 8.1 Defaults
- **Microsoft Account**
  - Kerb: Yes
  - Hashes: Yes
  - Plaintext-Equivalent Passwords: No

- **Local Account**
  - Kerb: Yes
  - Hashes: Yes
  - Plaintext-Equivalent Passwords: No

- **Domain Account**
  - Kerb: Yes
  - Hashes: Yes
  - Plaintext-Equivalent Passwords: No

### Windows 8.1 Features
- **Protected Users**
  - Kerb: Yes
  - Hashes: Yes
  - Plaintext-Equivalent Passwords: Yes

- **Restricted Admin RDP**
  - Kerb: Yes
  - Hashes: Yes
  - Plaintext-Equivalent Passwords: Yes

* Off by Default

---

Based on a table by Benjamin Delpy

twitter.com/gentilkiwi/status/352557093640892416/photo/1
Debug Privilege
DEMO

LSA dump using Mimikatz
Proactive Measures

- Restrict administrative access
- Applocker/SRP whitelisting
- Enable Additional LSA Protection
- Protected Users group
- Restricted Admin RDP
- Authentication Policies and Silos
- Shorten Kerberos ticket lifetime
- Disable Automatic Restart Sign-On
Automatic Restart Sign-On

Sign-in last interactive user automatically after a system-initiated restart

Options:
- Not Configured
- Enabled
- Disabled

Supported on:
At least Windows Server 2012 R2, Windows 8.1 or Windows RT 8.1

Help:
This policy setting controls whether a device will automatically sign-in the last interactive user after Windows Update restarts the system.

- If you enable or do not configure this policy setting, the device securely saves the user’s credentials (including the user name, domain and encrypted password) to configure automatic sign-in after a Windows Update restart. After the Windows Update restart, the user is automatically signed-in and the session is automatically locked with all the lock screen apps configured for that user.

- If you disable this policy setting, the device does not store the user's credentials for automatic sign-in after a Windows Update restart. The user's lock screen apps are not restarted after the system restarts.
Kerberos Ticket Lifetime
Tier Model

Tier 0

Tier 1

Tier 2
Tier Model - Administrative logon restrictions
High-Value Accounts

- **Admins**
  - Domain Admins
  - Enterprise Admin
  - Schema Admins
  - BUILTIN\Administrators
  - BUILTIN\Hyper-V Administrators

- **Service Accounts**
  - SCCM, SCOM, DPM, Software Installation,…

- **BMC Accounts**
Authentication Policies and Silos

Restrict Access for Admins

- General
  - Display name: Restrict Access for Admin
  - Description:
  - Protect from accidental deletion
  - Only audit silo policies
  - Enforce silo policies

- Permitted Accounts

- Authentication Policy
  - Use a single policy for all principals that belong to this authentication policy silo.

User

- Specify a Ticket Granting Ticket lifetime for user accounts:
  - Ticket Granting Ticket Lifetime (minutes): 600

- Specify access control conditions that restrict devices that can request a Ticket Granting Ticket for the user accounts assigned to this policy.

- Note: NTLM authentication cannot be restricted by access control conditions. Users should be members of the 'Protected Users' group, which does not allow NTLM.

Click Edit to define the conditions.

- Member of any(((W8-CONTOSO1S-WB1\W8_CONTOSO1S)))

Click Edit to define the conditions.

All Resources

Other user

Your account is configured to prevent you from using this PC. Please try another PC.
Credential Verifiers

- Windows caches AD credentials locally
- Used when DC is unavailable
- Defaults: 25 on servers, 10 on clients
- AKA MS-CACHE and MS-CACHE v2
MS-CACHE Algorithm (XP)

Password -> UTF-16 -> NT Hash

MD4

Login

Concat

MD4

Password Verifier
MS-CACHE v2 Algorithm (Vista+)

Password → NT Hash
  → UTF-16
    → MD4
      → MS-CACHE
        → MD4
          → Concat
            → Login
              → Password Verifier
                → PBKDF2
                  (HMAC-SHA1, 10240)
Configuring Credential Cache
Credentials Lifecycle / Attack Vectors

- Admin Password!
- External storage
- Sign-on
- Use/Cache on client
- In transit on network
- Authoritative store
Using the Hash/Key/Ticket
DEMO

Passing the NT hash using Mimikatz
Golden Ticket

kbereros::golden
/domain:chocolate.local
/sid:S-1-5-21-130452501-2365100805-3685010670
/aes256:15540cac73e94028231ef86631bc47bd5c827847ade468d6f6f739eb00c68e42
/user:srvcharly$
/id:1001
/groups:513,1107
/ticket:fake_utilisateur.kirbi
Proactive Measures

- Disable NTLM Authentication
- Disable Kerberos RC4-HMAC
- Implement Smartcard Authentication
- Unique local Administrator passwords
- Logon restrictions with new well-known SIDs
  - NT AUTHORITY\Local account
  - NT AUTHORITY\Local account and member of Administrators group
  - KB2871997 required on Windows 7 and 8

- Firewalls
Strengthening Kerberos Security
PtH Mitigation Strategies
Planning for compromise

- Identify all high-value assets
- Protect against known and unknown threats
- Detect PtH and related attacks
- Respond to suspicious activity
- Recover from a breach
NIST Framework for Improving Critical Infrastructure Cybersecurity
## NIST Framework for Improving Critical Infrastructure Cybersecurity

<table>
<thead>
<tr>
<th>Functions</th>
<th>Categories</th>
<th>Subcategories</th>
<th>Informative References</th>
</tr>
</thead>
<tbody>
<tr>
<td>IDENTIFY</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PROTECT</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DETECT</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RESPOND</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RECOVER</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
PtH Detection
Attack Graph

ELAPSED TIME: 8 HRS OR LESS
GET CREDENTIALS
Malicious tactics such as social engineering and phishing schemes are used to trick personnel and obtain credentials for network access. Most organizations do not recognize when attackers are already within the network and have access to information such as emails, confidential documents, and other intellectual property.

ELAPSED TIME: 24 HRS OR LESS
GET DATA
The attack doesn't stop there. Attackers look for the next set of credentials with elevated permissions to access servers. Once elevated credentials are obtained and servers are compromised, organizations risk losing revenue, brand reputation, and business continuity.

ELAPSED TIME: 48 HRS OR LESS
GET CONTROL
The ultimate goal of the attacker may be to gain access to the domain controllers, the central clearing hub for all credentials and identities. Once compromised, an attacker has complete control over an entire organization. All assets, intellectual property, physical property, and personal information are in jeopardy.
Events

- Authentication
  - Success
  - Failure
- Replication Traffic
- …
Audit Process Creation

<table>
<thead>
<tr>
<th>Subcategory</th>
<th>Audit Events</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit DPAPI Activity</td>
<td>Not Configured</td>
</tr>
<tr>
<td>Audit Process Creation</td>
<td>Success</td>
</tr>
<tr>
<td>Audit Process Termination</td>
<td>Not Configured</td>
</tr>
<tr>
<td>Audit RPC Events</td>
<td>Not Configured</td>
</tr>
</tbody>
</table>
Audit Process Creation
Audit Process Creation
Reactive Measures

- Change account passwords
- Reset computer account passwords
- Disable+Enable smartcard-enforced accounts
- Reset KRBTGT account
- Implement countermeasures
Windows 10
# New Challenges Require a New Platform

<table>
<thead>
<tr>
<th>Windows 7</th>
<th>Windows 10</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Identity protection</strong></td>
<td><strong>A viable alternative to passwords arrives</strong></td>
</tr>
<tr>
<td>Passwords theft increasingly successful</td>
<td>Easy and cost effective multi-factor</td>
</tr>
<tr>
<td>Multi-factor solutions too complex</td>
<td>A common solution everyone</td>
</tr>
<tr>
<td><strong>Data protection</strong></td>
<td><strong>Disk encryption increasingly enabled OOB</strong></td>
</tr>
<tr>
<td>Disk encryption difficult to deploy</td>
<td>DLP in Windows, better with Azure and Office</td>
</tr>
<tr>
<td>Use of 3rd party solutions DLP</td>
<td></td>
</tr>
<tr>
<td><strong>Threat resistance</strong></td>
<td><strong>Rate of new malware threats per day irrelevant</strong></td>
</tr>
<tr>
<td>300K’s+ malware new threats per day</td>
<td>Lock down Windows to only run trusted apps</td>
</tr>
<tr>
<td>No way for AV to keep up</td>
<td></td>
</tr>
<tr>
<td><strong>Security Hardware</strong></td>
<td><strong>Hardware protects system integrity</strong></td>
</tr>
<tr>
<td>Unable to maintain system integrity</td>
<td>Defenses isolated away from malware</td>
</tr>
<tr>
<td>Malware tampers with defenses and hides</td>
<td></td>
</tr>
</tbody>
</table>

- Windows Hello
- Microsoft Passport
- BitLocker
- Enterprise Data Protection
- Device Guard
- Windows Defender
- UEFI Secure Boot
- TPM 2.0, Virtualization
Hypervisor Code Integrity (HVCI) protected by VSM

- Virtual Secure Mode (VSM)
  - Local Security Auth Service
  - Virtual TPM
  - Hyper-Visor Code Integrity

- Kernel

- Windows

- Apps

- Hypervisor

- Hardware
Enables a Windows desktop to be locked down to only run trusted apps, just like many mobile OS’s (e.g.: Windows Phone)

Untrusted apps and executables such as malware are unable to run

Resistant to tampering by an administrator or malware

Requires devices specially configured by either the OEM or IT
DEVICE GUARD

Getting Apps into the Circle of Trust

Supports all apps including Universal and Desktop (Win32)

Trusted apps can be created by IHV, ISV, and Organizations using a Microsoft provided signing service

Apps must be specially signed using the Microsoft signing service. No additional modification is required

Signing service will be made available to OEM’s, IHV, ISV’s, and Enterprises
MICROSOFT PASSPORT

YOUR DEVICE IS ONE OF THE FACTORS

USER CREDENTIAL
An asymmetrical key pair
Provisioned via PKI or created locally via Windows 10

SECURED BY HARDWARE
Hello Chris

Fingerprint
Iris
Facial

WINDOWS
HELLO
Pass-the-Hash Attacks

Michael Grafnetter
www.dsinternals.com
Aktuální a navazující kurzy sledujte na www.gopas.cz

DÁREK PRO VÁS!

Vyplňte dotazníkové hodnocení a...

...získejte tričko TechEd-DevCon 2015!

TechEd party!
Billiard klub Harlequin Praha, 20.5.2015

SOUTĚŽ! SOUTĚŽ! SOUTĚŽ!

Bud'te The Best IT Pro
nebo The Best Developer