Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 79 (2016) 755 – 764

Procedia Computer Science

7th International Conference on Communication, Computing and Virtualization 2016

Implementation and mitigation of various tools for pass the hash attack

Navjyotsinh Jadeja[a]*, Viral Parmar[b]

[a,b]*Marwadi Education Foundation,Rajkot, Gujarat*

Abstract

Advances in computing technology is acquainting numerous colossal changes with individuals' way of life and working example as of late for its countless advantages. In any case, the security of cloud computing and server level technologies is dependably the center of various potential clients, and a major obstruction for its far-reaching applications. This paper introduces a novel approach of testing various tools that can be used to measure the potential helplessness of a digital system to particular sorts of assaults that uses lateral movement and privileged heightening, such as Pass The Hash. Earlier papers have only done the comparison at limited resources and have failed to show accurate result. While other papers and assets concentrate fundamentally on running the tools and in some cases contrasting them, this paper offers a top to bottom, orderly examination of the apparatuses over the different Windows stages, including AV discovery rates. It additionally gives broad counsel to moderate pass the hash assaults and talks about the upsides and downsides of a portion of the methodologies.

Keywords: Cloud security; hash attack; network security; Pass the hash attack

1. Introduction

Advancing technology and device which come along with that, the computing needs of the users are going up at rate of knots. Every computing service provider is facing the greatest challenge in terms of providing the security to its end user, protect data theft and many more. Security architectures and plans are implemented at various level to adhere to such standards. But still there exists mechanisms and ways where security can be compromised at the user

* Navjyotsinh Jadeja. M: +91- 9687194293.
E-mail address: noon2night88@gmail.com

doi:10.1016/j.procs.2016.03.099

level. This in turn can affect system as a whole. There are several existing attacks which affect the computing world everyday on big scale. One of such attacks is pass the hash attacks.

Although pass the hash attack in not a new form of attack. It has been around 18 years now since coming into forefront. There are various kinds of research conducted to reduce its severity and mitigate it, but the threat still looms over computing world. In this paper we discuss and extensively elaborate various tools used in different lab setup environment which helps in understanding and preventing the attacks to several levels.

2. Pass-the-hash attack

Password hashes can be directly used as a clear-text password[7], as the authentication process is comparison between hashes. If attacker can gain the access of the hash of the password, there won't be any need to get password. This type of attack is known is "Pass-the-hash attack". Once the user has logged in a system, the password hash is stored into Local Security Authority Subsystem (Lsass). Lsass runs as executable %SystemRoot%\system32\Lsass.exe, which handles the authentication and identification process in operating system. These password hashes can be dumped by attacker, using hash dump tools.

The process, in general, has a flow as given below[8]:

- The attacker dumps the hashes from the system to be accessed.
- By using pass-the-hash tools, attacker can place the obtained hashes into the local Lsass.
- Now whenever the attacker will try to access the server, he will be given new credentials, without need of providing password.

This attack is less time consuming than other attacks (i.e. password guessing, password cracking).

2.1. Methodology

There are various tools available for gaining the hashes or dumping the hashes from victim's system. All these tools were tested on various operating system based on windows framework, with and without Anti-Virus tools.

Tested tools are as listed below:

- Pwdump7
- Windows credentials Editor (wce)
- Corelab pass-the-hassh toolkit/ pshtoolkit
- Fgdump

These tools were tested in lab configuration.

2.2 Lab Setup

The lab was setup with multiple computers, having various versions of windows operating systems. It included four systems which are Windows 7 32/64-bit, Windows 8.1 64-bit, Windows 10 64-bit.

Anti-Virus installed for this purpose were:

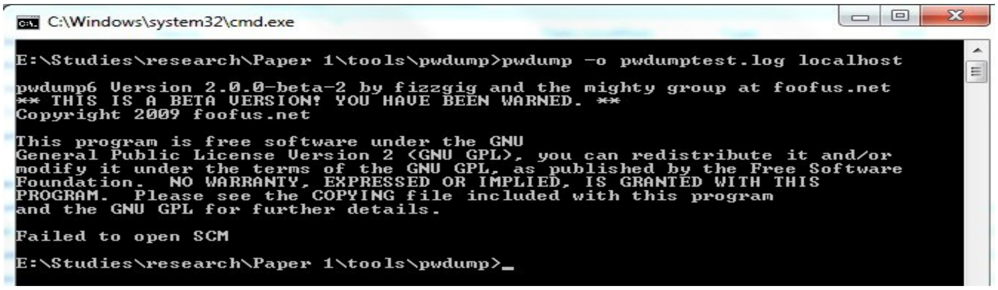
- Bit Defender (Paid)
- Microsoft Essential Security (MSE) (Free)
- AVG Antivirus (free)

Bit defender was selected because of its high ratings in best antivirus of the year 2015. MSE was used because it was inbuilt and had positive results so far and AVG was selected to test this threat against free antiviruses.

2.3. Attack: Pass-the-hash tool comparison

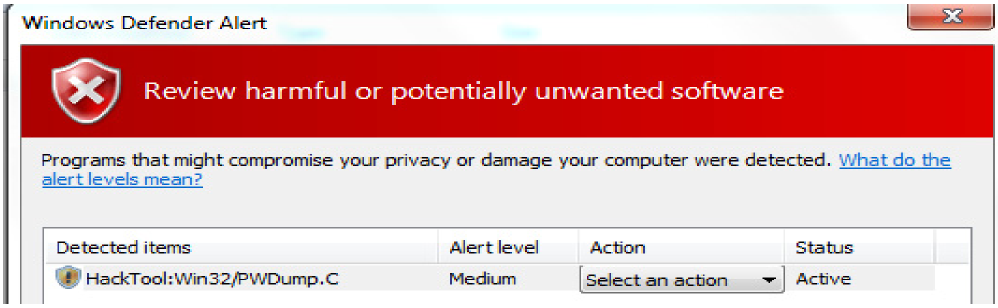
2.3.1. pwdump

pwdump is used to dump the hashes of the stored passwords LanMan and NTLM hashes as well as password hash histories can be dumped by this tool.[10].



```
E:\Studies\research\Paper 1\tools\pwdump>pwdump -o pwdumptest.log localhost

pwdump6 Version 2.0.0-beta-2 by fizzgig and the mighty group at foofus.net
** THIS IS A BETA VERSION! YOU HAVE BEEN WARNED. **
Copyright 2009 foofus.net

This program is free software under the GNU
General Public License Version 2 (GNU GPL), you can redistribute it and/or
modify it under the terms of the GNU GPL, as published by the Free Software
Foundation.  NO WARRANTY, EXPRESSED OR IMPLIED, IS GRANTED WITH THIS
PROGRAM.  Please see the COPYING file included with this program
and the GNU GPL for further details.

Failed to open SCM

E:\Studies\research\Paper 1\tools\pwdump>_
```

Fig. 1. Working of pwdump

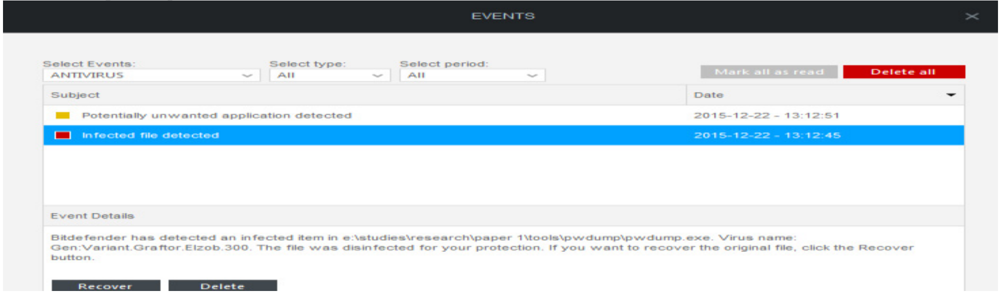


Review harmful or potentially unwanted software

Programs that might compromise your privacy or damage your computer were detected. What do the alert levels mean?

Detected items	Alert level	Action	Status
HackTool:Win32/PWDump.C	Medium	Select an action	Active

Fig. 2. MSE detection of pwdump.exe



Select Events: ANTIVIRUS
Select type: All
Select period: All

Subject	Date
🟨 Potentially unwanted application detected	2015-12-22 - 13:12:51
🟥 Infected file detected	2015-12-22 - 13:12:45

Event Details

Bitdefender has detected an infected item in e:\studies\research\paper 1\tools\pwdump\pwdump.exe. Virus name: Gen:Variant.Graftor.Elzob.300. The file was disinfected for your protection. If you want to recover the original file, click the Recover button.

Fig. 3. Bit defender detection of pwdump.exe

Table 1. Summary of lab test for pwdump.exe

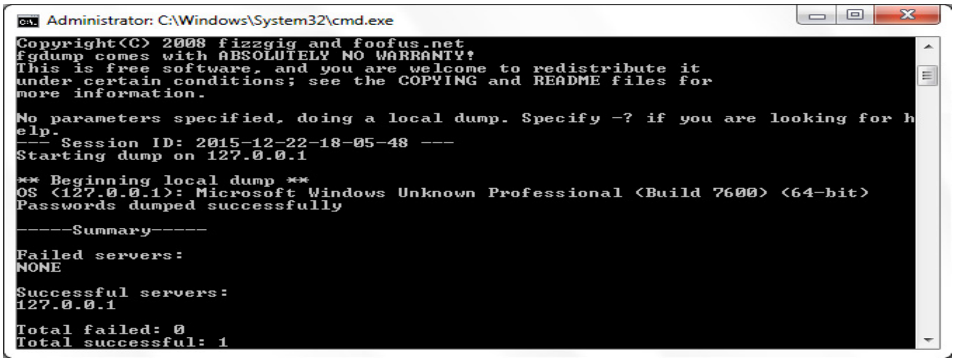
	Windows			
Name of Operating System	Windows 7 32-bit	Windows 7 64-bit	Windows 8.1 64-bit	Windows 10 64-bit
Results	Success	Failed	Failed	Failed

Table 2. Summary of lab test for pwdump.exe AV detection

pwdump.exe			
Name of AV	Bit defender	MSE	AVG
Results	Detected	Detected	Detected

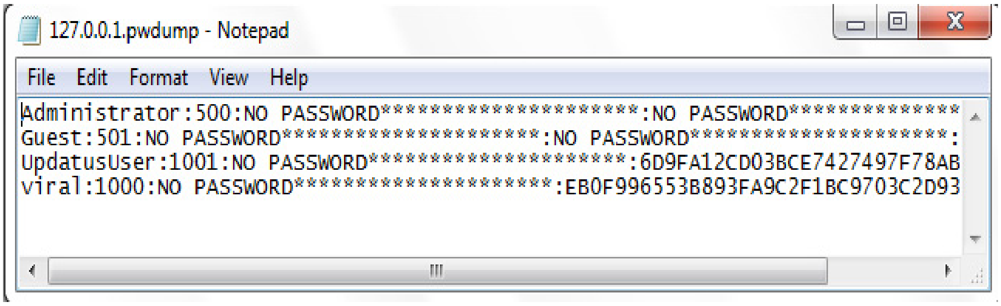
2.3.2. fgump

fgdump can be considered as a better version of pwdump[11]. Major difference between pwdump and fgdump is that pwdump leads to a crash when Anti-Virus is present where fgdump first tries to shut down the Anti-Virus and then runs its script. Cached credentials and protected storage items can also be dumped. Multithreading task is also easy with this.



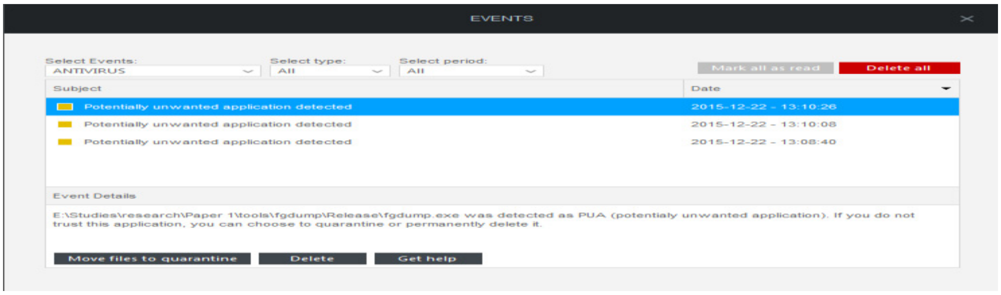
```
Copyright(C) 2008 fizzgig and foofus.net
fgdump comes with ABSOLUTELY NO WARRANTY!
This is free software, and you are welcome to redistribute it
under certain conditions; see the COPYING and README files for
more information.

No parameters specified, doing a local dump. Specify -? if you are looking for h
elp.
--- Session ID: 2015-12-22-18-05-48 ---
Starting dump on 127.0.0.1

** Beginning local dump **
OS (127.0.0.1): Microsoft Windows Unknown Professional (Build 7600) (64-bit)
Passwords dumped successfully

-----Summary-----

Failed servers:
NONE

Successful servers:
127.0.0.1

Total failed: 0
Total successful: 1
```

Fig. 4. Working of fgdump



```
Administrator:500:NO PASSWORD*********************:NO PASSWORD**************
Guest:501:NO PASSWORD*********************:NO PASSWORD*********************:
UpdatusUser:1001:NO PASSWORD*********************:6D9FA12CD03BCE7427497F78AB
viral:1000:NO PASSWORD*********************:EB0F996553B893FA9C2F1BC9703C2D93
```

Fig. 5.pwdump file created as output



Subject	Date
Potentially unwanted application detected	2015-12-22 - 13:10:26
Potentially unwanted application detected	2015-12-22 - 13:10:08
Potentially unwanted application detected	2015-12-22 - 13:08:40

Event Details

E:\Studies\research\Paper 1\tools\fgdump\Release\fgdump.exe was detected as PUA (potentialy unwanted application). If you do not trust this application, you can choose to quarantine or permanently delete it.

Fig. 6. Bit defender detection of fgdump.exe

Table 3. Summary of lab test for fgdump.exe

		Windows		
Name of OS	Winodws 7 32-bit	Windows 7 64-bit	Windows 8.1 64-bit	Windows 10 64-bit
Results	Success	Failed	Failed	Failed

Table 4. Summary of lab test for fgdump.exe AV detection

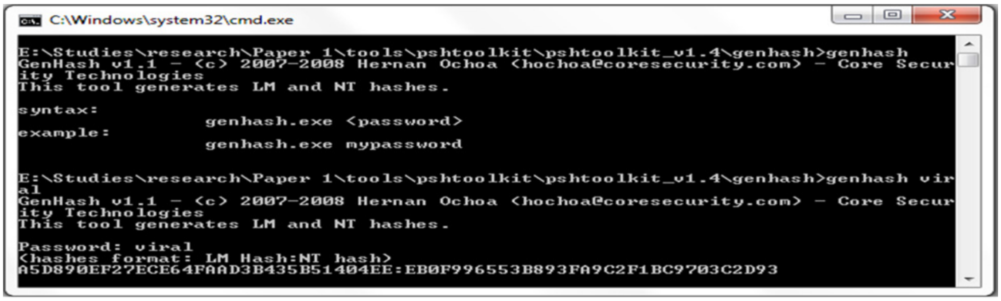
		fgdump.exe	
Name of AV	Bit defender	MSE	AVG
Results	Detected	Not Detected	Not Detected

2.3.3. pshtoolkit

By this tool, current logon sessions with their corresponding NTLM credentials can be listed. Changes in the current username, domain name and NTLM hashes can be made runtime by this tool[9]. Utilities to make changes in windows logon sessions are contained by this toolkit.

2.3.3.1. genhash

genhash utility is used for generating hash code of given text[9]. This tool doesn't require any administrative privileges to run. In output it provides LM and NT hashes for given text. This utility can be used on any system based on Microsoft framework.

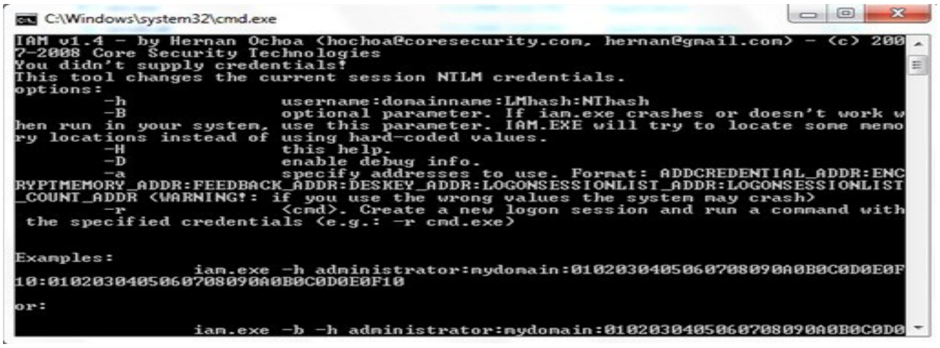


```
E:\Studies\research\Paper 1\tools\pshtoolkit\pshtoolkit_v1.4\genhash>genhash
GenHash v1.1 - (c) 2007-2008 Hernan Ochoa (hochoa@coresecurity.com) - Core Secur
ity Technologies
This tool generates LM and NT hashes.

syntax:
                genhash.exe <password>
example:
                genhash.exe mypassword


E:\Studies\research\Paper 1\tools\pshtoolkit\pshtoolkit_v1.4\genhash>genhash vir
al
GenHash v1.1 - (c) 2007-2008 Hernan Ochoa (hochoa@coresecurity.com) - Core Secur
ity Technologies
This tool generates LM and NT hashes.

Password: viral
(hashes format: LM Hash:NT hash)
A5D890EF27ECE64FAAD3B435B51404EE:EB0F996553B893FA9C2F1BC9703C2D93
```

Fig. 7. Working of genhash

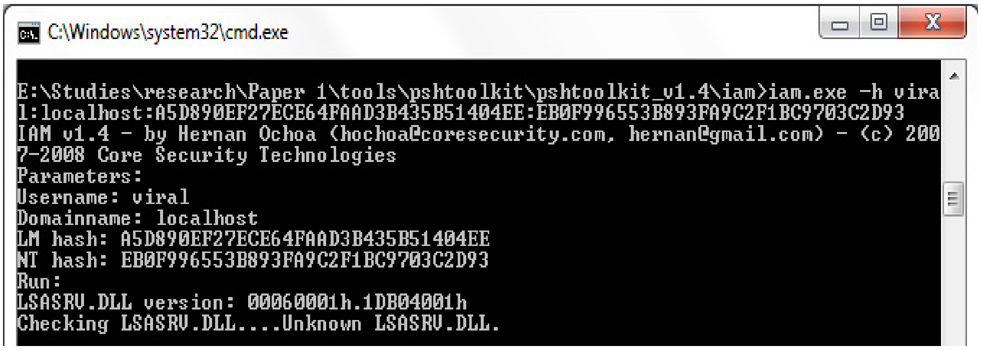
2.3.3.2. iam and iam-alt

These tools can be used to change current NTLM credentials by using hashes directly[9]. In output, username, domain name and LM and NT hashes are given by these tools. After making changes in the credentials all the connections will use new credentials, which are modified by iam, for the authentication.



```
IAM v1.4 - by Hernan Ochoa (hochoa@coresecurity.com, hernan@gmail.com) - (c) 200
7-2008 Core Security Technologies
You didn't supply credentials!
This tool changes the current session NTLM credentials.
options:
        -h              username:domainname:LMhash:NThash
        -B              optional parameter. If iam.exe crashes or doesn't work w
hen run in your system, use this parameter. IAM.EXE will try to locate some memo
ry locations instead of using hard-coded values.
        -H              this help.
        -D              enable debug info.
        -a              specify addresses to use. Format: ADDCREDENTIAL_ADDR:ENC
RYPTMEMORY_ADDR:FEEDBACK_ADDR:DESKEY_ADDR:LOGONSESSIONLIST_ADDR:LOGONSESSIONLIST
_COUNT_ADDR (WARNING!: if you use the wrong values the system may crash)
        -r              (cmd). Create a new logon session and run a command with
 the specified credentials (e.g.: -r cmd.exe)


Examples:
                iam.exe -h administrator:mydomain:0102030405060708090A0B0C0D0E0F
10:0102030405060708090A0B0C0D0E0F10

or:

                iam.exe -b -h administrator:mydomain:0102030405060708090A0B0C0D0
```

Fig. 8. Help menu of iam.exe



```
E:\Studies\research\Paper 1\tools\pshtoolkit\pshtoolkit_v1.4\iam>iam.exe -h vira
l:localhost:A5D890EF27ECE64FAAD3B435B51404EE:EB0F996553B893FA9C2F1BC9703C2D93
IAM v1.4 - by Hernan Ochoa (hochoa@coresecurity.com, hernan@gmail.com) - (c) 200
7-2008 Core Security Technologies
Parameters:
Username: viral
Domainname: localhost
LM hash: A5D890EF27ECE64FAAD3B435B51404EE
NT hash: EB0F996553B893FA9C2F1BC9703C2D93
Run:
LSASRV.DLL version: 00060001h.1DB04001h
Checking LSASRV.DLL....Unknown LSASRV.DLL.
```

Fig. 9. Failure of iam.exe

Table 5. Summary of lab test for iam.exe

	Windows			
Name of OS	Winodws 7 32-bit	Windows 7 64-bit	Windows 8.1 64-bit	Windows 10 64-bit
Results	Failed	Failed	Failed	Failed

Table 6. Summary of the lab test for iam.exe AV detection

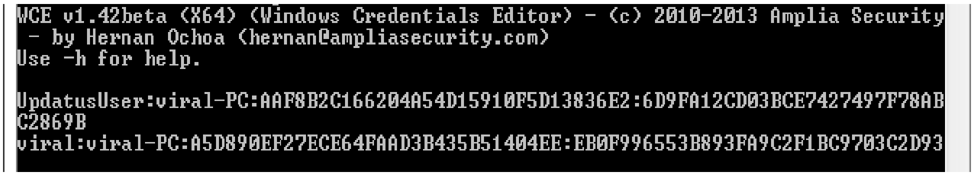
	iam.exe		
Name of AV	Bit defender	MSE	AVG
Results	Detected	Not Detected	Detected

2.3.3.3. whosthere and whosthere-alt

This tools lists logon sessions with username, domain name, LM and NT hashes[9]. This can be used at time when some system is compromised but it’s not main system. Now usually, admins access such systems remotely, at that time attacker can use this tool to gain access to admin’s credentials and then use them with iam and get access of main server. Wrong or faulty addresses ,if used, can crash the whole system.

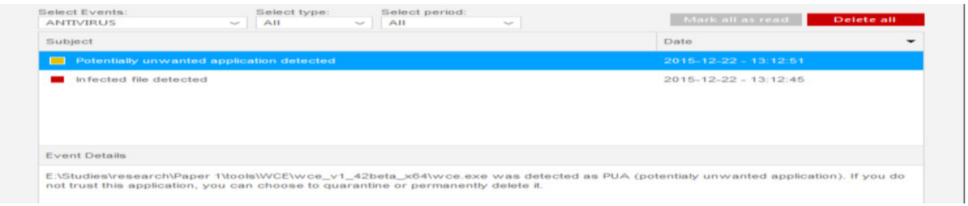
2.3.4. Windows Credentials Editor (WCE)

By this tool, list of windows logon session can be generated and furthermore, attacker can make changes in provided credentials. This tool can also be used to gain Kerberos tickets from windows framework based systems. Cleartext passwords stored by WAP can also be dumped by this tool.



```
WCE v1.42beta (X64) (Windows Credentials Editor) - (c) 2010-2013 Amplia Security
 - by Hernan Ochoa (hernan@ampliasecurity.com)
Use -h for help.

UpdatusUser:viral-PC:AAF8B2C166204A54D15910F5D13836E2:6D9FA12CD03BCE7427497F78AB
C2869B
viral:viral-PC:A5D890EF27ECE64FAAD3B435B51404EE:EB0F996553B893FA9C2F1BC9703C2D93
```

Fig.10. Working of WCE



Select Events: ANTIVIRUS
Select type: All
Select period: All

Subject	Date
🟨 Potentially unwanted application detected	2015-12-22 - 13:12:51
🟥 Infected file detected	2015-12-22 - 13:12:45

Event Details

E:\Studies\research\Paper 1\tools\WCE\wce_v1_42beta_x64\wce.exe was detected as PUA (potentialy unwanted application). If you do not trust this application, you can choose to quarantine or permanently delete it.

Fig.11. Bit defender detection of WCE.exe

Table 7. Summary of the lab test for wce.exe

		Windows		
Name of Operating System	Winodws 7 32-bit	Windows 7 64-bit	Windows 8.1 64-bit	Windows 10 64-bit
Results	Success	Success	Success	Success

Table 8. Summary of the lab test for wce.exe AV detection

		wce.exe	
Name of AV	Bit defender	MSE	AVG
Results	Detected	Not Detected	Not Detected

3. Pass-the-hash defense

One of the reasons why this attack is implementable is ‘vulnerability of windows’ unsalted password hashing mechanism’. But, as the hash is equivalent to the clear text password, it can’t be blocked even by using salting. One of the assumptions made earlier was attacker already has the administrative rights in victim’s system. If that can be secured, then multiple attacks including pass-the-hash can be mitigated.

This section will cover the points and precautions by which organization can build secure and reliable system from such attacks.

3.1. Disjoint data

As we saw earlier, it becomes very hazardous for an organization if an attacker can get access to the password hashes in the main domain controller, leading him to have full control over domain. An attacker can dump the password hashes using tools and then use them with iam or whosthere and then using output details with tools like iam can lead them to have full access to the domain.

That’s why there is very important rule that:
"A more sensitive system must never depend on a less sensitive system for its security.”

That leads us to:

- Systems which are not trust worthy or system which are less secure, should not be allowed to manipulate the data which is more important than system itself.
- The admin should not directly login to any system using root credentials. If there is need for admin to connect to a system then a temporary admin account can be used and should be deleted after completion of purpose.
- Systems used for setting up temporary connections, should be trusted and designated for specific purpose.

3.2. Least User Access (LUA)

As the attack can be implemented through unintentional malicious activity by admin, the risk increases with more number of admins. Organization can defend their systems from such scenarios by applying Least User Access approach given by Microsoft. A study shows that 92% threats can be solved by implementing this approach. There are many users who has admin rights but they never use them. In this approach, admin rights are revoked from these users. Even though this approach is not implementable in all circumstances and all systems but it reduces the risk to drastic amount in systems in which it is implemented.

3.4. Avoid support to less secure protocols or remove backward compatibility

LM and NTLM challenge-response have been outdated now and should not be supported. A suggestible approach is NTLMv2 or Kerberos because of their flow of communicating with server from client is more secure. This can be done by changing group policies in DC and client. This setting is made of basically 2 commands:

- What client should offer?
- What DC should accept?

The best setting for this policy would be "Send NTLMv2 response only/refuse LM and NTLM". By this policy, client could only send NTLMv2 responses and DC will only accept NTLMv2 and rejects LM as well as NTLM.

Windows 7 comes with undefined policy and LMCompatibilityLevel in the registry can also be set by administrators to enforce the type of client responses and behavior of DC upon those responses through:

HKLM\SYSTEM\CurrentControlSet\Control\Lsa\LMCompatibilityLevel

3.4. Decrease the limit of Cached Credentials

Cached credentials come in handy to users when they are facing lost connectivity. If the cached credentials applied, all the users' data will be cached without a doubt. The default number of credentials cached in windows versions is 25 except windows 2008, which provides allowance of 10 cached credentials.

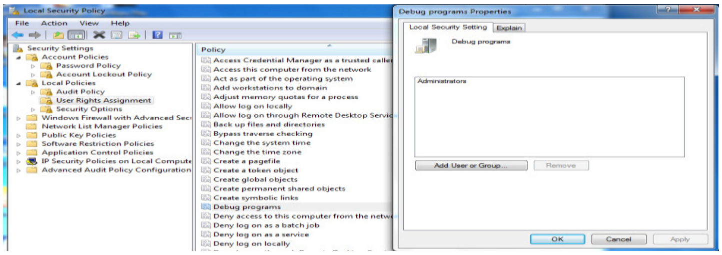
Use of same passwords is done by some organizations. Because of this, if one system is compromised then attacker will get all the info and credentials of a user from that compromised system and in will be in no time when attacker will have access to main domain. To defend system from this risk, cached credentials should be set on 0 for desktops and servers and 1 for laptops. It can be changed by making changes in registry given below

HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\Current Version\Winlogon\

In the scenario where clusters are used, different values are preferable as setting it to 0 may crash the cluster nodes.

3.5. Revoking user right "Debug Programs"

Even if user doesn't own the process, a debugger can be attached to that process (i.e. kernel) by the user. This is known as "Debug Programs" user right. This provides access to sensible data to users which don't need it. This right can be exploited by attackers by tools which are used to dump hashes and merge them with any process. Then it becomes easy when a user with administrative right runs that process, the dump of passwords is made by that tool attached to it. This right doesn't have much importance from users' perception but it becomes risk when exploited by attacker and that is why it should be revoked. If system has "cluster service" running, then stopping or revoking this right will fail that service and that is why it is necessary to keep Debug Programs user right when system has "cluster service". It can be changed from local policies as shown in the figure 12, given below:


Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Firewall with Advanced Secu
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration
Policy
Access Credential Manager as a trusted caller
Access this computer from the network
Act as part of the operating system
Add workstations to domain
Adjust memory quotas for a process
Allow log on locally
Allow log on through Remote Desktop Servic
Back up files and directories
Bypass traverse checking
Change the system time
Change the time zone
Create a pagefile
Create a token object
Create global objects
Create permanent shared objects
Create symbolic links
Debug programs
Deny access to this computer from the netwo
Deny log on as a batch job
Deny log on as a service
Deny log on locally
Debug programs Properties
Local Security Setting
Explain
Add User or Group...
Remove
OK
Cancel
Apply

Debug programs

Administrators

Fig.12. Modifying "Debug Programs" user right

Noticeable result after revoking this user right is, this caused mostly all tools to fail except pwdump and fgdump.

3.6. Token based authentication

Implementation of token based authentication is complex and costly, which makes it hard to implement in many organizations. In 2004, Microsoft and RSA announced SecureID for windows. Pseudo-random six digits' number, based on hardware, was generated by this as a token. This number is displayed on device for specific duration of time, which will be asked to user on time of login, for authentication. This makes it hard for an attacker to gain access of the system without its physical access, i.e. from the remote system.

3.7. Kerberos and Smart Cards

This configuration can provide a reliable security to reply attacks or attacks which target the access of sensible information offline. Storage of information in DC for smartcard is same as passwords. When smart card is used for login, random password created by DC for this card will be hashed and stored in user object. When smart card is used for login after that, KDC provides user's hash to client during the login procedure. Encryption is done on this message using the public key of the client. On the other hand, client side, the hash will be decrypted and cached as if user entered credentials at login prompt by Kerberos Security Support Provider. When unreachable to Kerberos, this credentials will be used by one computer to silently sign into another. The risk of exposure of client side's hashes, to malicious attacks, still remains same.

3.8. NIDS and HIDS monitoring

If intrusion detection is set up on both systems and network, then the security increases for the malicious attack or activity. This includes multiple operations on host and networks. Monitoring the host on regular short intervals for recent activities on accounts and local administrator group memberships. Output gained from this analysis should be compared to other outputs gained in previous analyses and if any suspicious account found then it should be deleted and alert should be sent. There are tools to monitor systems (i.e. snare agent) and forward alerts for reporting to other system (ex. Splunk system). Sending alert when the Event 552 is shown in event viewer, which indicates that explicit contents were used from another system or account. Few tools like fgdump, shuts down the antivirus before running its script and it makes system vulnerable. To avoid that, there should be some script which will only monitor on Anti-virus programs and if they behave abnormally then report an alert or restart or start the service if they are stopped unexpectedly. At the end, system must be free of anomalies. For example, making too many connections in short time and same port.

4. Conclusion

The attack exposes the underlying design flaw in Microsoft's password hashing algorithms and their implementation. Due to availability of free and easy tools which can help an attacker to make a pass-the-hash attack, this attack could get very dangerous. Getting access of hash can give whole access of the network or domain controller to the attacker which could lead to disastrous event. To prevent that from happening, organizations should take proper steps including monitoring hosts, network, traffic and abnormalities. As well as emphasizing on implementing Least User Access. Also can refer to various methods suggest in earlier papers by us[4].

Table 9. Comparison between different tools

Comparison Factor	pwdump	fgdump	pshtoolkit	WCE
Successful results in Windows 7 32-bit	✓	✓	×	✓
Successful results in Windows 7 64-bit	×	✓	×	✓
Successful results in Windows 8.1 64-bit	×	✓	×	✓

Successful results in Windows 10 64-bit	×	×	×	✓
Detected by Bit Defender AV	✓	✓	✓	✓
Detected by AVG AV	✓	×	✓	×
Detected by MSE	✓	×	✓	×

This attack mainly depends on whether attacker can gain administrative privileges or not. That is why servers and controllers should not be allowed to be accessed by all users or all systems. It should only be allowed to be accessed by trusted systems with no internet connections. Even though there will be more threats in future and penetration for defense methods will be discovered, but to keep system safe, organizations should keep updating their security on regular basis. As a part of future work, we suggest to improve the overall system architecture from security perspective. Backward compatibility for weak protocols like LM and NTLM shouldn’t be allowed. Authentication processes, which use two-way tokens, are highly recommended to avoid these attacks. An exhaustive arrangement tending to physical, network, and host based security must be executed to give satisfactory levels of assurance.

References

[1] Johnson, J.R.; Hogan, E.A., "A graph analytic metric for mitigating advanced persistent threat," in Intelligence and Security Informatics (ISI), 2013 IEEE International Conference, vol., no., pp.129-133, 4-7 June 2013.

[2] Vukalovic, J.; Delija, D., "Advanced Persistent Threats - detection and defense," in Information and communication Technology, Electronics and Microelectronics (MIPRO), 2015 38th International Convention, vol., no., pp.1324-1330, 25-29 May 2015.

[3] Groat, S.; Tront, J.; Marchany, R., "Advancing the defense in depth model," in System of Systems Engineering (SoSE), 2012 7th International Conference, vol., no., pp.285 -290, 16-19 July 2012.

[4] Navjyotsinh Jadeja, Madhuri Vaghasia, “Analysis and Impact of Different Mechanisms of Defending Pass the Hash Attacks” in CSI 2015, International Conference, Springer Proceeding, 2-5 Dec 2015.

[5] Johansson, J. (2009). Windows Server 2008 Security. Rockland: Syngress Publishing Inc.

[6] Scambray, J. & McClure, S. “Hacking Exposed: Windows” 3 rd ed. New York: McGraw-Hill (2008).

[7] BeyondTrust. “New Report Shows 92 Percent of Critical Microsoft Vulnerabilities are Mitigated by Eliminating Admin Rights” Retrieved January 2, 2010, from BeyondTrust Web site: http://pm.beyondtrust.com/company/pressreleases/03Feb2009.aspx

[8] Metzler, D. “Part1: Adventures in NTLM Pass-The-Hash Mitigation” Retrieved July 5,2009, from Confessions of Technoholic Website: http://metzlertech2.spaces.live.com/Blog/cns!BB9E1D7036F624E9!126.

[9] Core Security “What is Pass-The-Hash Toolkit” Retrieved August 30, 2009, from Core Security. Website: http://oss.coresecurity.com/projects/pshtoolkit.htm

[10] Foofus “Whats is pwdump” Retrieved January 29, 2009, from foofus . website: http://foofus.net/goons/fizzgig/pwdump/

[11] Foofus “Whats is fgdump” Retrieved September 18, 2008, from foofus. website: http://foofus.net/goons/fizzgig/fgdump/

[12] Ampila Security “Whats is windows credentials editor, from Ampila security”. website:http://www.ampliasecurity.com/research/windows-credentials-editor/