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.

Peer-review under responsibility of the Organizing Committee of ICCCV 2016

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

Peer-review under responsibility of the Organizing Committee of ICCCV 2016
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.