metasploit® pro

Pass the Hash

Quick Start Guide

Pass the hash is an attack method that attempts to use a looted password hash to authenticate to a remote system. It enables you to use a raw hash, which means that you do not need to decrypt the hash or know the plain text password. This attack method makes it very easy to compromise other machines that share the same credentials.

If you are able to obtain an NTLM password hash during your penetration test, you can run the Pass the Hash MetaModule. It attempts to use the Windows file and print sharing service, which operates over a protocol known as Server Message Block (SMB), to authenticate to other hosts in the network.

In order to run the Pass the Hash MetaModule, you must have a looted credential pair that consists of a raw NTLM hash and the associated user name. A password hash can be obtained from a compromised host by running evidence collection, by manually browsing a file system to locate the Security Accounts Manager (SAM), or by dumping the password hashes. Once you have a valid credential pair, you only need to specify the target hosts that you want the MetaModule test the credentials against.

During the MetaModule run, Metasploit Pro displays real-time statistics for the number of hosts targeted, the number of login attempts made, and the number of successful logins. You can quickly identify the hosts that share the same login as the host from which you obtained the NTLM hash. You can leverage this information to move laterally across the network or to escalate your privileges to gain access to higher value machines.

When the MetaModule completes its run, it generates a complete report that provides the details for the hosts it was able to successfully authenticate. You can share this report with your organization to expose weak and shared passwords and to help mitigate vulnerabilities in its security infrastructure.

Product Terms

MetaModule	A feature that extends the capabilities of modules in Metasploit Pro to perform penetration testing tasks.
Password Hash	A unique string of data generated by cryptographic algorithms to encrypt a plain text password.
Pass the Hash	A method of attack that uses a looted password hash to access other systems on a network.
Pass the Hash MetaModule	A MetaModule that identifies systems that can be authenticated with a looted password hash.

Before You Begin

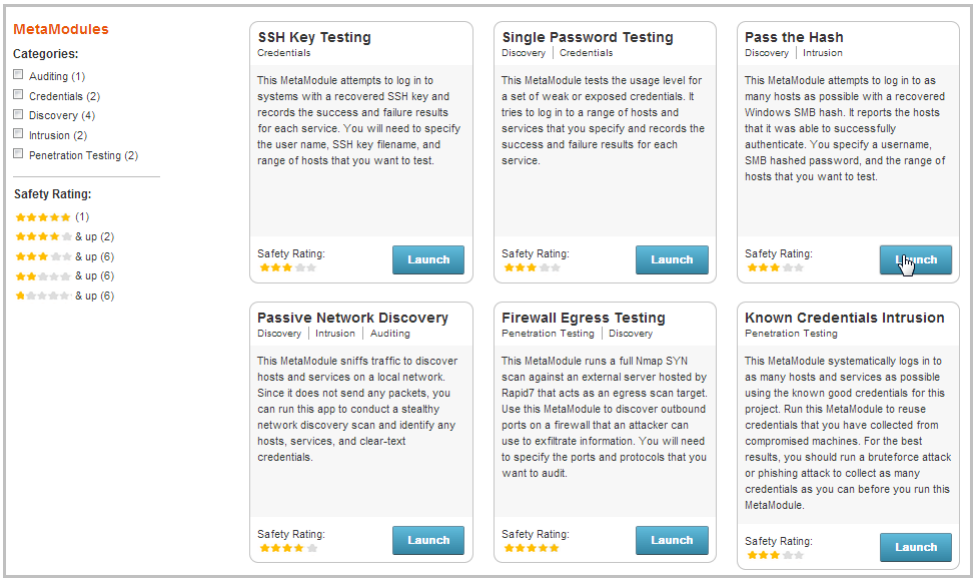
Clear Your Browser's Cache	After you install or update Metasploit, you must clear your browser's cache to ensure that all user interface elements load properly.
Loot an NTLM Hash	Before you can run the Pass the Hash MetaModule, you must either have a raw NTLM hash that you can manually input for the test or your project must contain an NTLM hash looted from a compromised system.

Last updated 07/17/2013 - 4.7

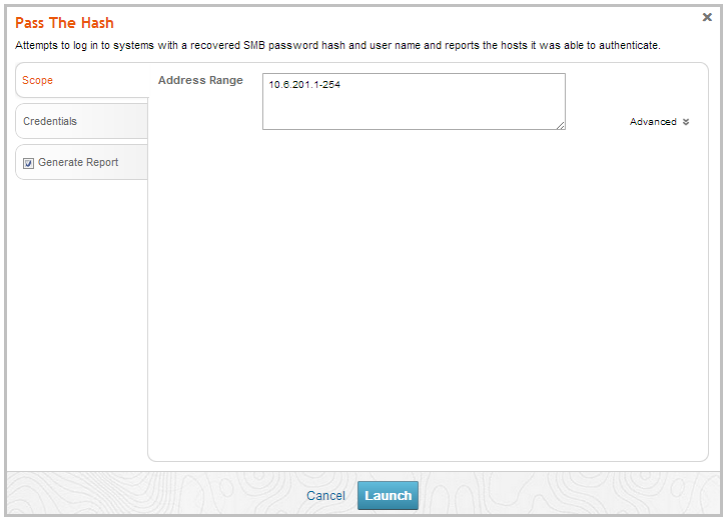
Passing the Hash

1. Log in to the Metasploit Pro web interface (https://localhost:3790).
2. Open the default project.
3. Select **Modules > MetaModules**.

4. Find the **Pass the Hash** MetaModule and click the **Launch** button. The **Pass the Hash** window appears.



5. From the **Scope** tab, enter the target address range you want to use for the test.

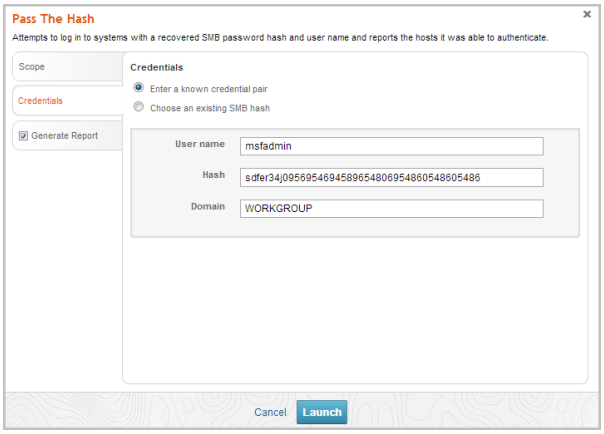


6. Click on the **Credentials** tab.

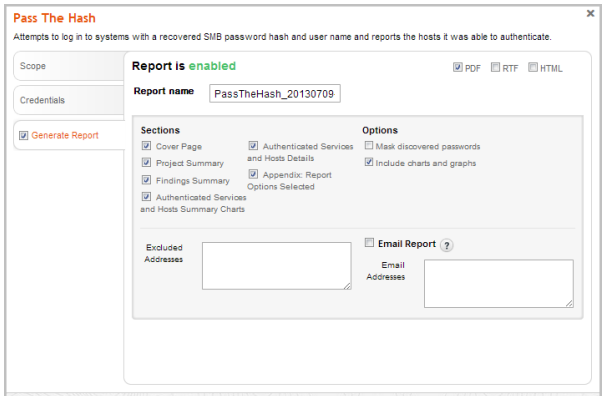
7. Choose one of the following options to supply the MetaModule with a raw NTLM hash:

   - **Enter a known credential pair** - You need to manually enter the user name, and then enter the raw hash that you want the MetaModule to use. You should leave `WORKGROUP` as the domain name in order to authenticate to the local machine.

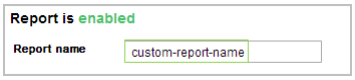
   - **Choose an existing SMB hash** - You can select a user name and hash from a list of looted password hashes that are stored in the project.



8. Click the **Generate Report** tab.



9. Enter a name for the report in the **Report Name** field, if you want to use a custom report name. Otherwise, the MetaModule uses the default report name.



10. Choose PDF, HTML, or RTF for the report format. PDF is the preferred format.

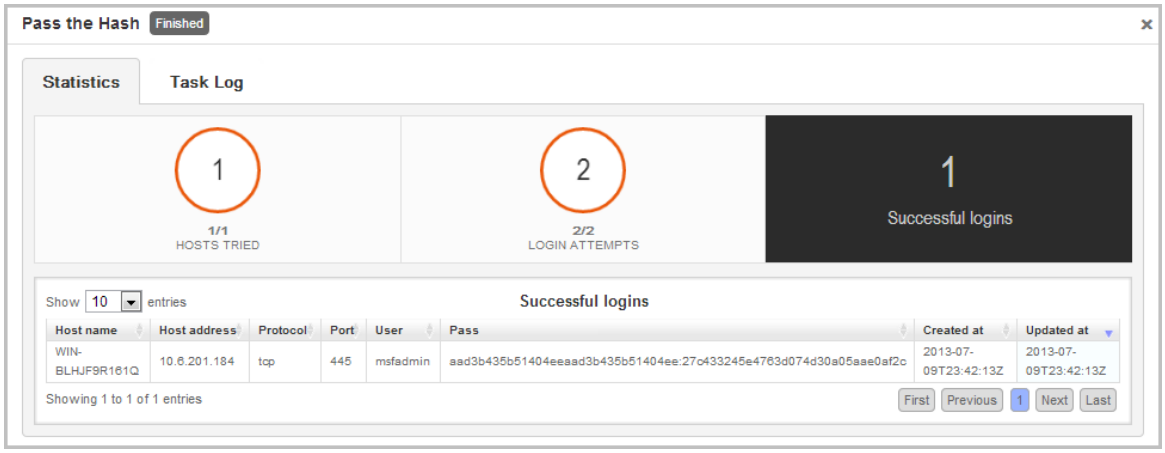
11. From the **Sections** area, deselect any sections you do not want to include in the report. Skip this step if you want to generate all the report sections.

12. Select the **Email Report** option if you want to e-mail the report after it generates. If you enable this option, you need to supply a comma separated list of e-mail addresses.

    Note: If you want to e-mail a report, you must set up a local mail server or e-mail relay service for Metasploit Pro to use. To define your mail server settings, select **Administration > Global Settings > SMTP Settings**.

13. Click the **Launch** button.

When the MetaModule launches, the Findings window appears and displays the real-time statistics and tasks log for the MetaModule run. You can track the total number of hosts that the MetaModule attempted to authenticate, the total number of login attempts, and the total number of successful logins. If you want to view all the event details, you can click on the **Task Log** tab.



After the MetaModule completes its run, you should go the Reports area to view the Pass the Hash Report. The first few pages of the report show graphs and tables that provide a high-level breakdown of cracked hosts and services. For a more detailed look at the hosts, you can look at the Authenticated Services and Hosts Details section, which shows the services that were authenticated and the sessions that were opened on each host.