metasploit® pro

SSH Key Testing

Quick Start Guide

SSH public key authentication provides a secure method of logging in to a remote host. It uses an SSH key pair to authenticate a login instead of the traditional user name and password combination. The SSH key pair consists of a private and public SSH key. The private SSH key is stored on the local machine and enables you to log in to remote systems on which the corresponding public key is installed.

If you obtain an unencrypted SSH private key from a compromised target machine, you can run the SSH Key Testing MetaModule. This MetaModule enables you to bruteforce logins on a range of hosts to identify remote machines that can be authenticated with the private key. 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. After the MetaModule completes its run, it generates a complete report that provides the details for the hosts it was able to successfully authenticate.

Product Terms

MetaModule	A feature that extends the capabilities of modules in Metasploit Pro to perform penetration testing tasks.
Private Key	A cryptographic key stored on a local machine that enables it to connect with a remote machine that has the corresponding public key.
Public Key	A cryptographic key installed on a remote machine that can be used to encrypt messages, which can only be deciphered with the private key.
Public Key Authentication	A secure method of authentication that uses a private and public key to verify a host's identity.
SSH Key Testing MetaModule	A MetaModule that attempts to bruteforce logins on a range of target hosts with a looted SSH private key.

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 a Private Key	Before you can run the SSH Key Testing MetaModule, you must either have a SSH private key available that you can upload to your project or your project must contain a looted SSH private key obtained from a scan, a bruteforce attack, or exploitation.
Run a Discovery Scan or Import Host Data	Before you can run the SSH Key Testing MetaModule, you must run a Discovery Scan on the target network range or import existing host data. This populates the project with the necessary host information, such as open ports and services, that the MetaModule needs to run.

Last updated 07/17/2013 - 4.7

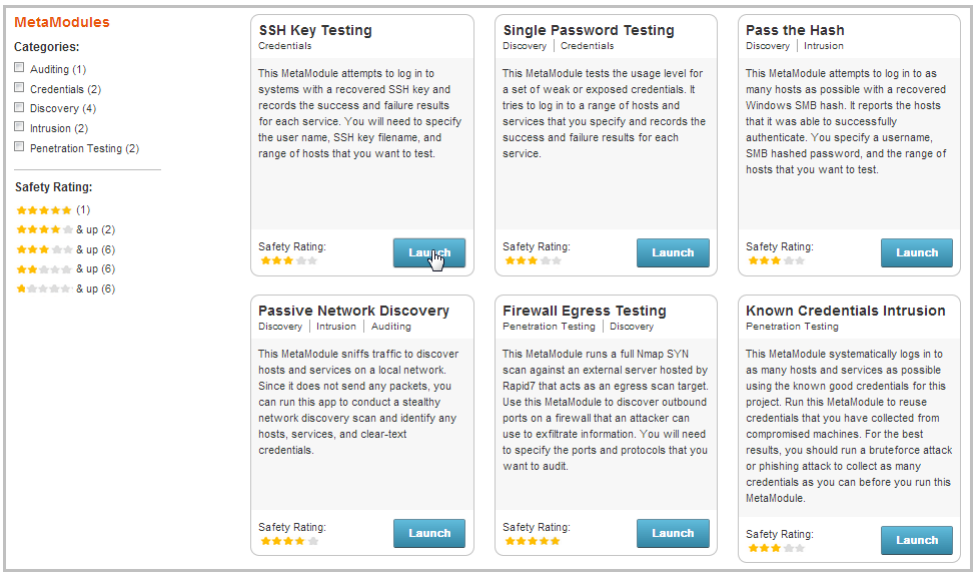
SSH Key Testing

1. Log in to the Metasploit Pro web interface (https://localhost:3790).

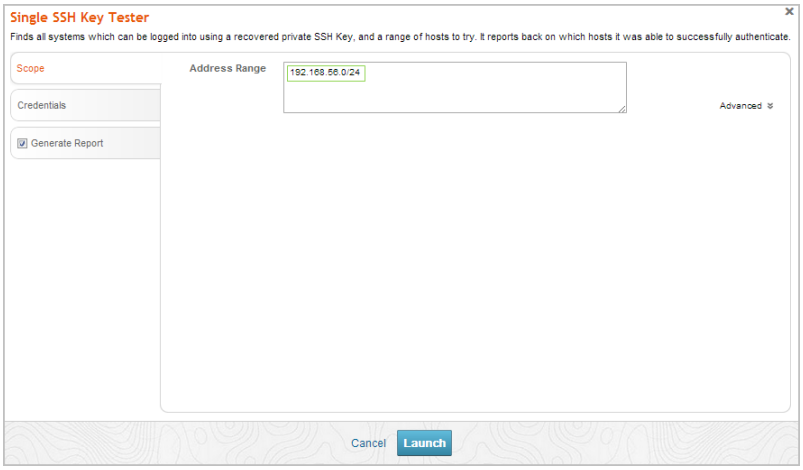
2. Open the default project.

3. Select **Modules > MetaModules**.

4. Find the **SSH Key Testing** MetaModule and click the **Launch** button. The **SSH Key Testing** window appears.



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

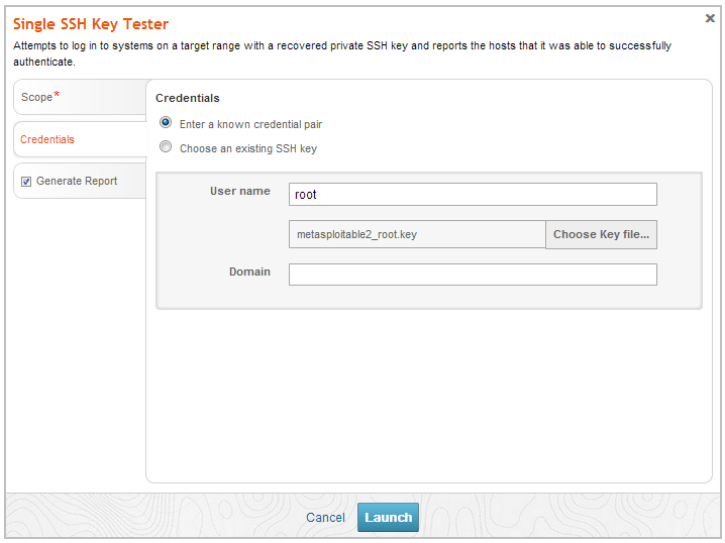


6. Click on the **Credentials** tab.

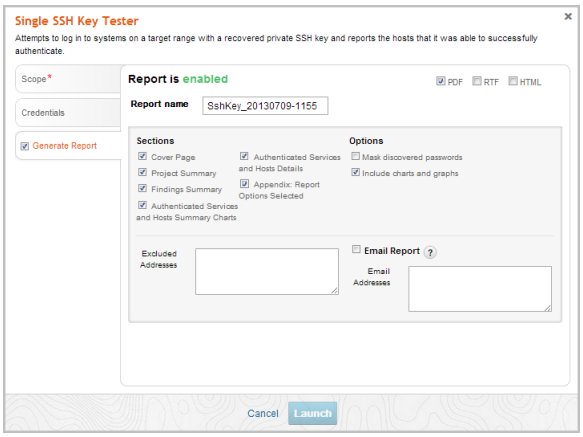
7. Choose one of the following options to supply the MetaModule with an SSH private key:

   - **Manually enter credentials** - You need to manually enter the user name, and then browse to the location of the private key that you want the MetaModule to use.

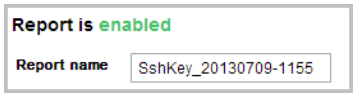
   - **Choose an existing SSH key** - You can select a user name and SSH key from a list of looted keys. These keys were obtained from a bruteforce attack, discovery scan, data import, or exploited system.



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.

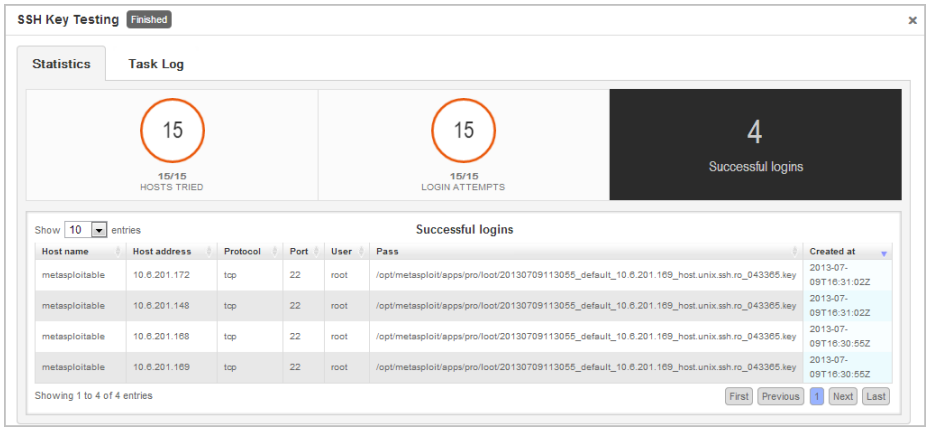
11. From the **Sections** area, deselect any sections you do not want to include in the report. Skip this step if you want to generate all the report sections.

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 SSH Key Testing 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.