metasploit® pro

Single Password Testing

Quick Start Guide

During a penetration test, you may need to demonstrate how password reuse could expose major weaknesses in an enterprise's security posture. A single cracked password can enable you to easily compromise other systems that share the same password.

The Single Password Testing MetaModule recycles a known credential pair to identify additional systems that can be authenticated. You can provide the MetaModule with a known credential pair that you've uncovered through a scan, bruteforce attack, or phishing attack.

When you configure this MetaModule, you need to define the services that you want to authenticate on your target hosts. The MetaModule attempts to log in to each service and records any successful login. After the MetaModule completes its run, it generates a report that details the hosts on which it was able to authenticate the credentials.

Product Terms

Credential	A user name and password combination.
Lockout Risk	The likelihood that a service enforces an account lockout.
MetaModule	A feature that extends the capabilities of modules in Metasploit Pro to perform penetration testing tasks.

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.
Run a Discovery Scan or Import Host Data	Before you can run the Single Password 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.

Lock Out Risk Categories

Low Risk	Any service that typically does not enforce account lockouts, such as AFP, DB2, EXEC, FTP, HTTP, HTTPS, LOGIN, Oracle, Postgres, SHELL, SNMP, SSH_PUBKEY, Telnet, and VNC.
Medium Risk	Any service that typically enforces account lockouts, such as MSSQL, MySQL, POP3, and SSH.
High Risk	Any service that uses Windows authentication, such as PC Anywhere, SMB, vmauthd, and WinRM.

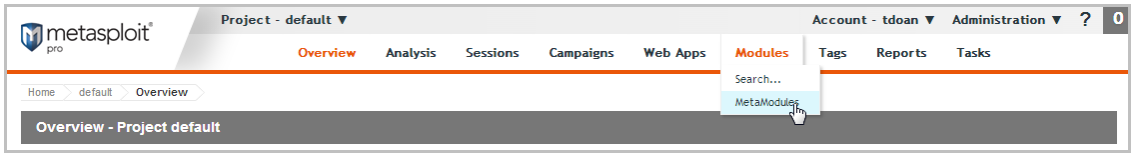
Last updated 07/17/2013 - 4.7

Single Password Testing

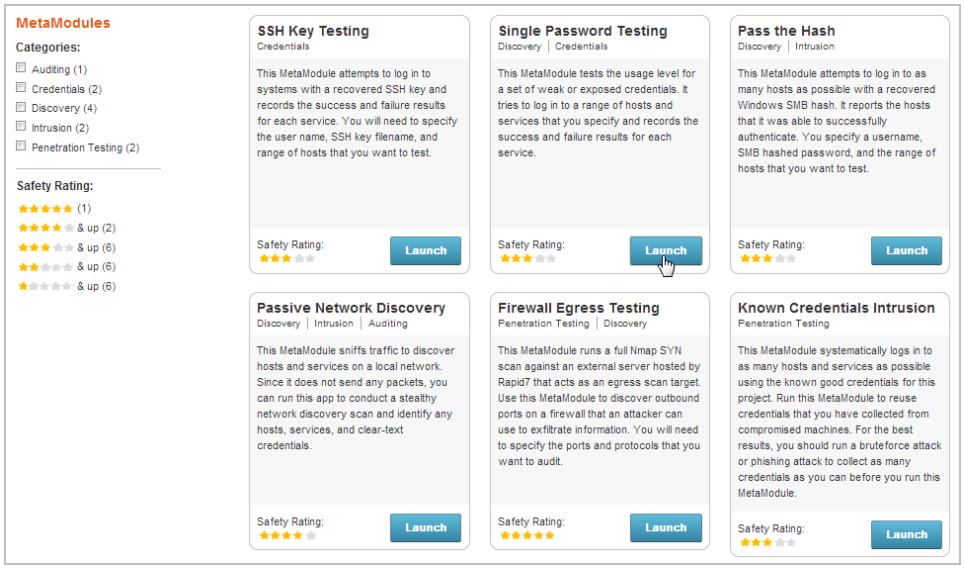
1. Log in to the Metasploit Pro web interface (https://localhost:3790).

2. Open the default project.

3. Select **Modules > MetaModules**.

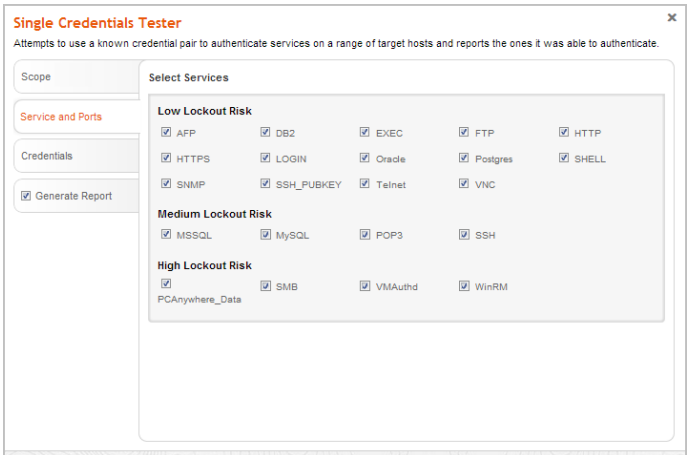


4. Find the **Single Password Testing** MetaModule and click the **Launch** button. The **Single Password Testing** window appears.



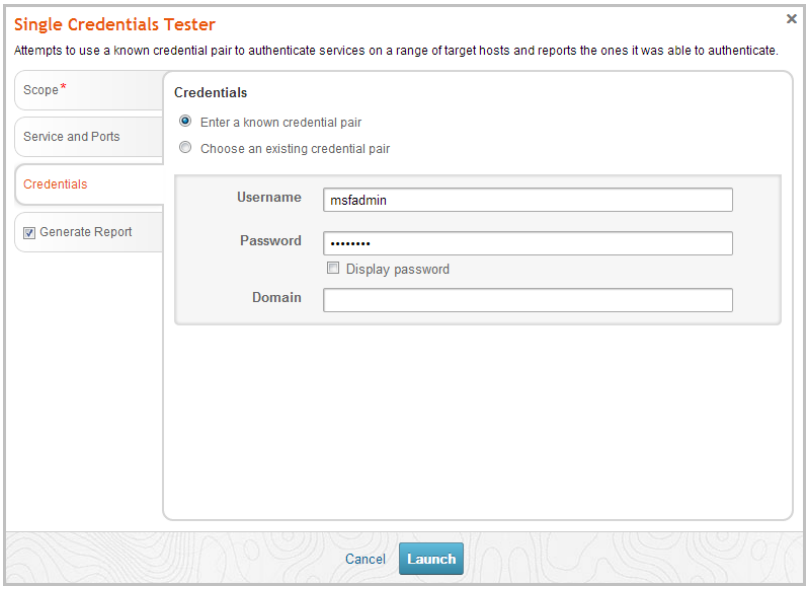
5. From the **Scope** tab, enter the target address range you want to use for the test. The target address range must match the hosts in the workspace.

6. Click on the **Services and Ports** tab.



7. Select the services that you want to attempt to authenticate. All services are categorized based on their lockout risk, which is the likelihood that the service locks an account after a number of failed logins.

8. Click on the **Credentials** tab.

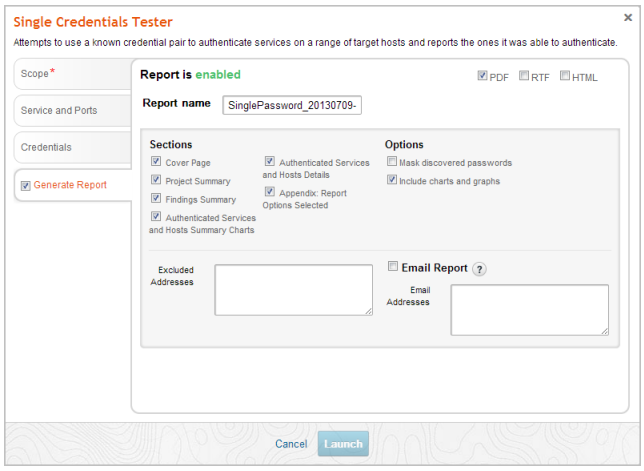


9. You can choose one of the following options to supply the MetaModule with credentials:

   - **Enter a known credential pair** - You need to manually enter the user name and password combination that you want the MetaModule to use. Use this method for credentials obtained from phishing attacks.

   - **Choose an existing credential pair** - You can select the user name and password combination from a list of known credentials. These credentials were obtained from a bruteforce attack, discovery scan, or data import.

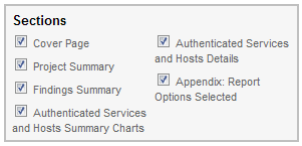
10. Click the **Generate Report** tab.



11. 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.

12. Select PDF, Word, RTF, or HTML for the report format. PDF is the preferred format.

13. 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.



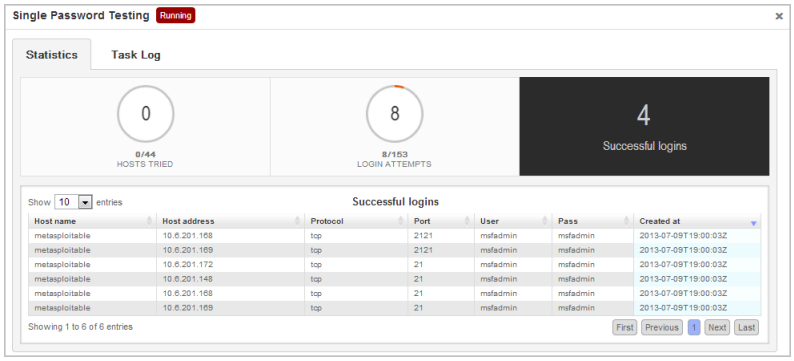
14. From the **Options** area, select the **Mask discovered passwords** option if you want to obscure any passwords that the report contains.

15. 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**.

16. 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 Single Password Testing Report. The first few pages of the report show graphs and tables that provide a high-level breakdown of authenticated services and hosts. For a more detailed look at the compromised 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.