Known Credentials Intrusion
Quick Start Guide

The Known Credentials Intrusion MetaModule logs in to a list of specified services and attempts to open sessions on a range of hosts with the known credentials in the project. You can run this MetaModule if you want to quickly get shells on the hosts in your project.

In order to run the Known Credentials Intrusion MetaModule, the project must already contain credentials that you have either collected from a Discovery Scan, bruteforce attack, or data import. The Known Credentials Intrusion MetaModule attempts to authenticate to each service that has been enumerated for each host. If the MetaModule is able to successfully log in to the service, it attempts to open a session on the target, which you can use to do things like set up a VPN pivot, collect system data, or launch a shell to interact with the target system. It opens one session per target, and it will move onto the next host in the test if a session has already been established for a host.

During the MetaModule run, Metasploit Pro displays real-time statistics for the number of hosts targeted and the number of sessions opened. When the MetaModule completes its run, it generates a complete report that provides the details for the hosts on which it was able to open a session. You can share this report with your organization to expose weak passwords and to help mitigate vulnerabilities in its security infrastructure.

Product Terms

Credential	A user name and password pair.
MetaModule	A feature that extends the capabilities of modules in Metasploit Pro to perform penetration testing tasks.
Known Credentials Intrusion MetaModule	A MetaModule that opens as many sessions as possible on a range of target hosts with all of the known credentials stored in the project.
Reverse Shell Payload	A payload that creates a connection from the target machine back to the attacking machine. If the target machines use NAT or is behind a firewall, then you should use a reverse shell payload.
Bind Shell Payload	A payload that binds a command prompt to a listening port on the target machine so that you can connect to it.
Payload	A piece of code that an exploit delivers to and executes on a target machine.
Listener	A component that waits for an incoming connection.

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 Known Credentials Intrusion 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.

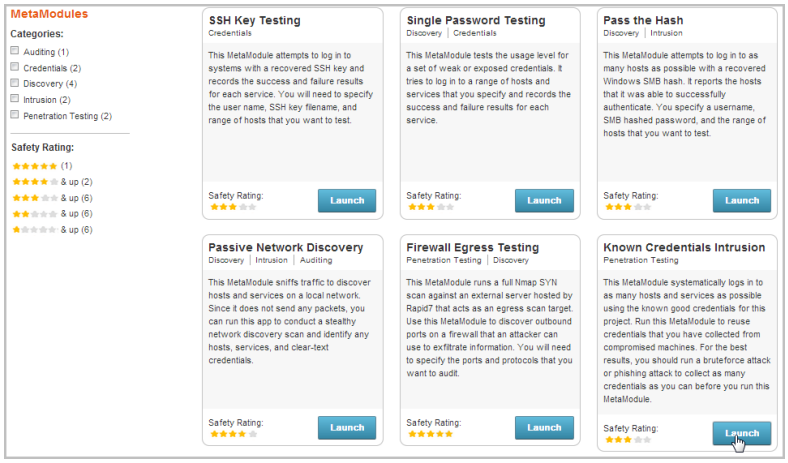
Last updated 07/17/2013 - 4.7

Before You Begin

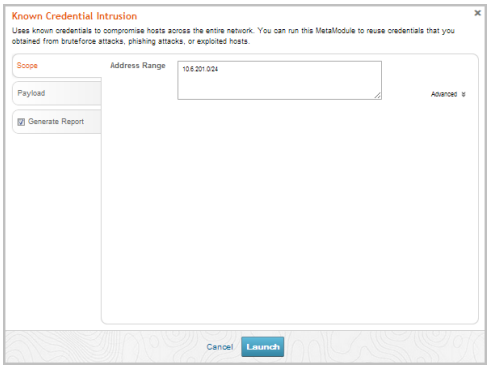
Loot Some Credentials	The project must contain credentials that you have looted from target hosts. There are multiple methods you can use to obtain credentials, including discovery scans, bruteforce attacks, automated exploitation, key loggers, password sniffing, and phishing attacks. For the purposes of this tutorial, the easiest way to steal credentials is to run an automated exploit run against your targets hosts, followed by a bruteforce attack. If you are able to establish a sessions on any host using one of these methods, you can run evidence collection to loot password files, such as password hashes and ssh keys.

Known Credentials Intrusion Testing

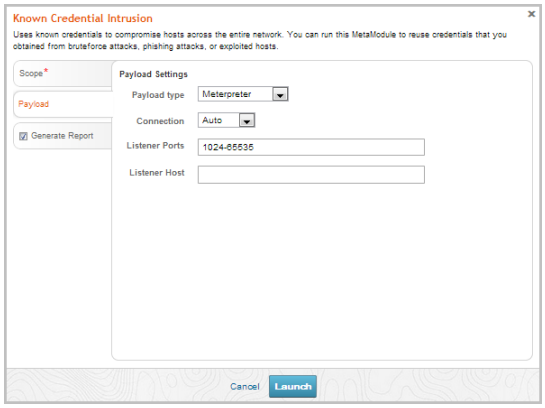
1. Log in to the Metasploit Pro web interface (https://localhost:3790).
2. Open the default project.
3. Select **Modules > MetaModules**.
4. Find the **Known Credentials Intrusion** MetaModule and click the **Launch** button. The **Known Credentials Intrusion** window appears.



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



6. Click on the **Payload** tab to configure the payload settings.

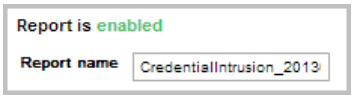


7. Specify the following settings that you want to use for the payload:

   - **Payload type** - Choose **Meterpreter** for Windows or **Command shell** for Linux systems.
   - **Connection** - Choose one of the following connection types:
     - **Auto** - Automatically selects the payload type. In most cases, the Auto option selects the reverse shell payload because it is more likely to establish a connection between a target machine and the attacking machine.
     - **Reverse** - Select this option if the targets are behind a firewall or use NAT. Typically, a reverse shell payload will work for most situations.
     - **Bind** - Select this option if the target devices are unable to initiate a connection.
   - **Listener Ports** - The port that you want the listener to listen on for incoming connections. By default, ports 1024-65535 are selected; however, you can define a specific port that you want the listener to use, such as 4444.
   - **Listener Host** - The IP address that you want the target machine to connect back to. This is typically going to be the IP address of your local machine. If you do not specify a listener host, the MetaModule automatically uses the IP address of your local machine.

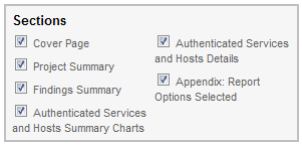
8. Click the **Generate Report** tab.

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.



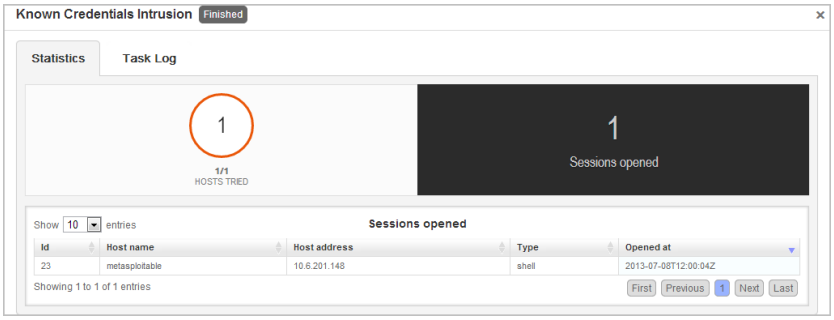
12. From the **Options** area, select the **Mask discovered passwords** option if you want to obscure any passwords that the report contains.

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

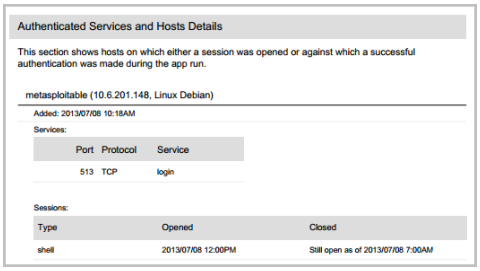
    If you want to e-mail a report, you must set up a local mail server or e-mail relay service for Metasploit Pro to use. To define your mail server settings, go to **Administration > Global Settings > SMTP Settings**.

14. Click the **Launch** button to start the MetaModule run.

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 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.



Once you are done with the test, you can go to the Sessions page to clean up and close any active sessions.