RAPID7

Metasploit Express

User Guide

Metasploit Express User Guide
Release 4.0
July 30, 2011

Table of Contents

About Metasploit Express

Metasploit Express is an easy-to-use penetration testing solution that provides network penetration testing capabilities, backed by the world's largest fully tested and integrated public database of exploits. Built on feedback from the Metasploit user community, key security experts, and Rapid7 customers, Metasploit Express enables organizations to take the next step forward in security.

Metasploit Express was designed for corporate security professionals, security consulting practices, and existing Metasploit users. If you already use the open-source Metasploit Framework to develop and test exploit code, you will appreciate the increased execution and browsing functionality of Metasploit Express.

In addition to the capabilities offered by the open source framework, Metasploit Express goes above and beyond by delivering a full graphical user interface, automated exploitation capabilities, complete user action audit logs, customizable reporting, combined with an advanced penetration testing workflow. Metasploit Express is fully supported by Rapid7 security and support specialists in addition to the large and growing Metasploit community.

Metasploit Express is a part of the Metasploit Project, the open-source penetration testing and development toolset for security professionals. The Metasploit Project was acquired by Rapid7 to continue the open-source community involvement, and to expand the project's capability and ease-of-use.

Metasploit Express can be installed on Windows and Linux machines and runs on almost any web browser, or you can continue to use the command line interface.

Metasploit Express Components Overview

Metasploit Express consists of four major components:

- The Metasploit Framework: The Metasploit Framework is both a penetration testing system and a development platform for creating security tools and exploits. The framework is written in Ruby and includes components in C and assembler. The framework consists of tools, libraries, modules, and user interfaces. The basic function of the framework is a module launcher, which allows the user to configure an exploit module and launch it at a target system.
- Express-Specific Modules – Metasploit Express contains the tasks (discover, bruteforce, etc.) functionality in the form of modules. These modules automate the functionality provided in the open source framework, and make it simpler to perform multiple related tasks.
- The Metasploit Express Workflow Manager – The Metasploit Express Workflow Manager is the logical component which provides the user with intelligent defaults, pen testing workflow, and module-specific guidance during the penetration test. The Metasploit workflow manager composes the pieces of the product that automate the individual modules. You could call this the "glue" that brings all the components together.

- Metasploit Express User Interface – In addition to the capabilities offered by the open source framework, Metasploit Express delivers a full graphical user interface, automated exploitation capabilities, complete user action audit logs, customizable reporting, combined with an advanced penetration testing workflow.

Metasploit Express Service Listeners

Metasploit Express is composed of the following services which interoperate to provide the Express interface:

- :3790 – Apache SSL Service – Metasploit Express utilizes Apache as a frontend web server for the Rails UI application. This is the primary service you will be interacting with when utilizing Metasploit Express.
- :3001 –Thin Rails Server (bound to localhost) – Metasploit Express utilizes Ruby on Rails, and Thin is used as the glue layer between Apache and Rails.
- :7337 – PostgreSQL Database (bound to localhost) – Metasploit Express uses PostgreSQL as the host for the datastore. PostgreSQL was chosen for performance reasons.
- :50505 – Metasploit RPC Service (bound to localhost) – The Metasploit Express Pro RPC service is similar to that provided with the open source framework, with additional functionality added. This service makes it possible to communicate directly with the Metasploit Express system via RPC. The Rails UI utilizes RPC on this port to communicate with the Metasploit Express engine.

About This Guide

This User Guide provides comprehensive information and instructions for Metasploit Express. The following sections will describe the audience, organization, and conventions used within this User Guide.

Target Audience

This User Guide is intended for IT and security professionals who use Metasploit Express as their penetration testing solution.

Organization

This User Guide is divided into the following chapters:

- Welcome
- About This Guide
- New Features in Metasploit Express
- Metasploit Express Interface Tour
- Getting Started with Metasploit Express
- Administration
- Metasploit Express Tasks
- Task Settings
- Supported Targets
- Warnings
- Index

Document Conventions

The following table lists the conventions and formats used within this User Guide.

Table 1: Document Conventions

Conventions	Description
Command	Text in this typeface indicates Metasploit Express buttons, options, features, and commands as well as filenames. For example, “Click **Forward** to continue” and “Locate the **Reports** tab”.

`Code`	Text in this typeface represents command line, file directory, or code. For example, `chmod +x Desktop/metasploit-3.7.1-linux-x64-installer.`
Title	Text in this typeface refers to document, chapter, and section names. For example, “For more information, see the *Metasploit Express User Guide*.”
Note:	Refers to additional information you may need to be aware of.

Support

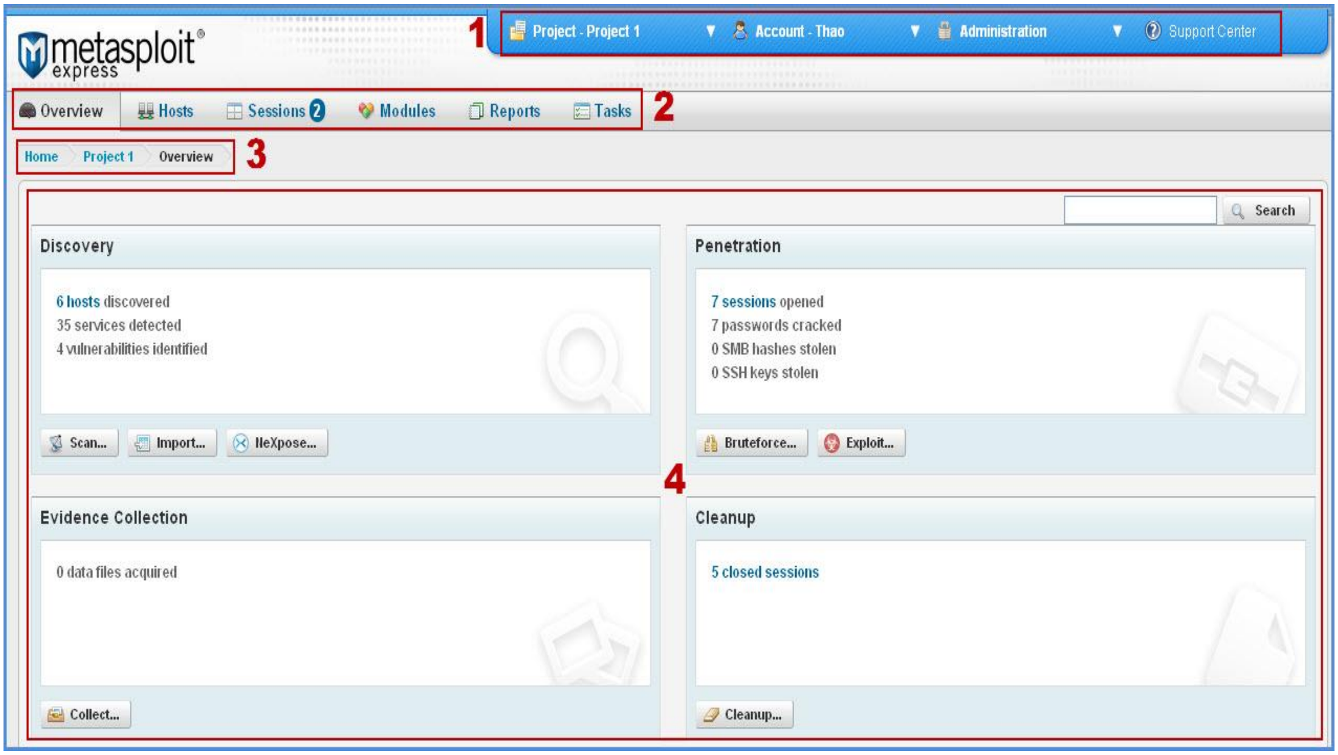
We are dedicated to delivering superior support for our products. Use the Customer Center to ask questions and get assistance for Metasploit Express. To log into the Customer Center, you will need to use the email and password you entered to create your account when you purchased Metasploit Express.

The Customer Center can be accessed at http://www.rapid7.com/customers/customer-login.jsp.

Metasploit Express Interface Tour

The following sections will provide you with a quick tour of the different areas within the user interface.

Navigational Tour



Discovery

6 hosts discovered
35 services detected
4 vulnerabilities identified

Penetration

7 sessions opened
7 passwords cracked
0 SMB hashes stolen
0 SSH keys stolen

Evidence Collection

0 data files acquired

Cleanup

5 closed sessions

Figure 1: Navigational Overview

There are five main areas of the interface that you can use to navigate through your project:

1. **Main Menu** – The Main menu enables you to manage your project settings, user account settings, and administration duties.
2. **Task Tabs** – The Task tabs enable you to navigate between individual Task pages. Task pages include Hosts, Sessions, Campaigns, Web Apps, Modules, Reports, and Tasks.
3. **Navigational Breadcrumbs** – The navigational breadcrumbs enable you to move, between Task pages. Typically, there will be three breadcrumbs listed (**Home > Project Name > Task Page**). Click on **Home** to access the **Projects** page.
4. **Dashboard** – The Dashboard provides you with a graphical breakdown of the services, operating systems and session statues running on the system. Additionally, you can run any of the main tasks from the Dashboard – including scans, exploits, and campaigns.
5. **Task Panes** – There are four Task panes that will always be visible to you from the Overview page: Discovery, Penetration, Web Apps, and Social Engineering. The Task buttons listed within each Task pane will apply that particular task to the entire project.

Projects Page Tour

To access the **Project** page, you can either click on the **Home** link located in the breadcrumbs or you can select **Projects > Show All Projects** from the Main menu.

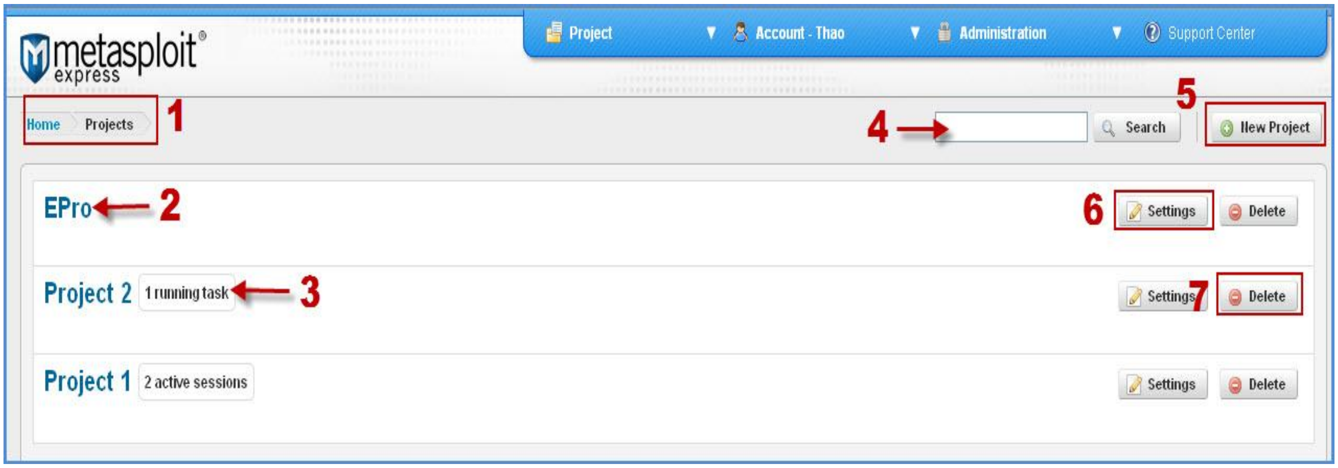


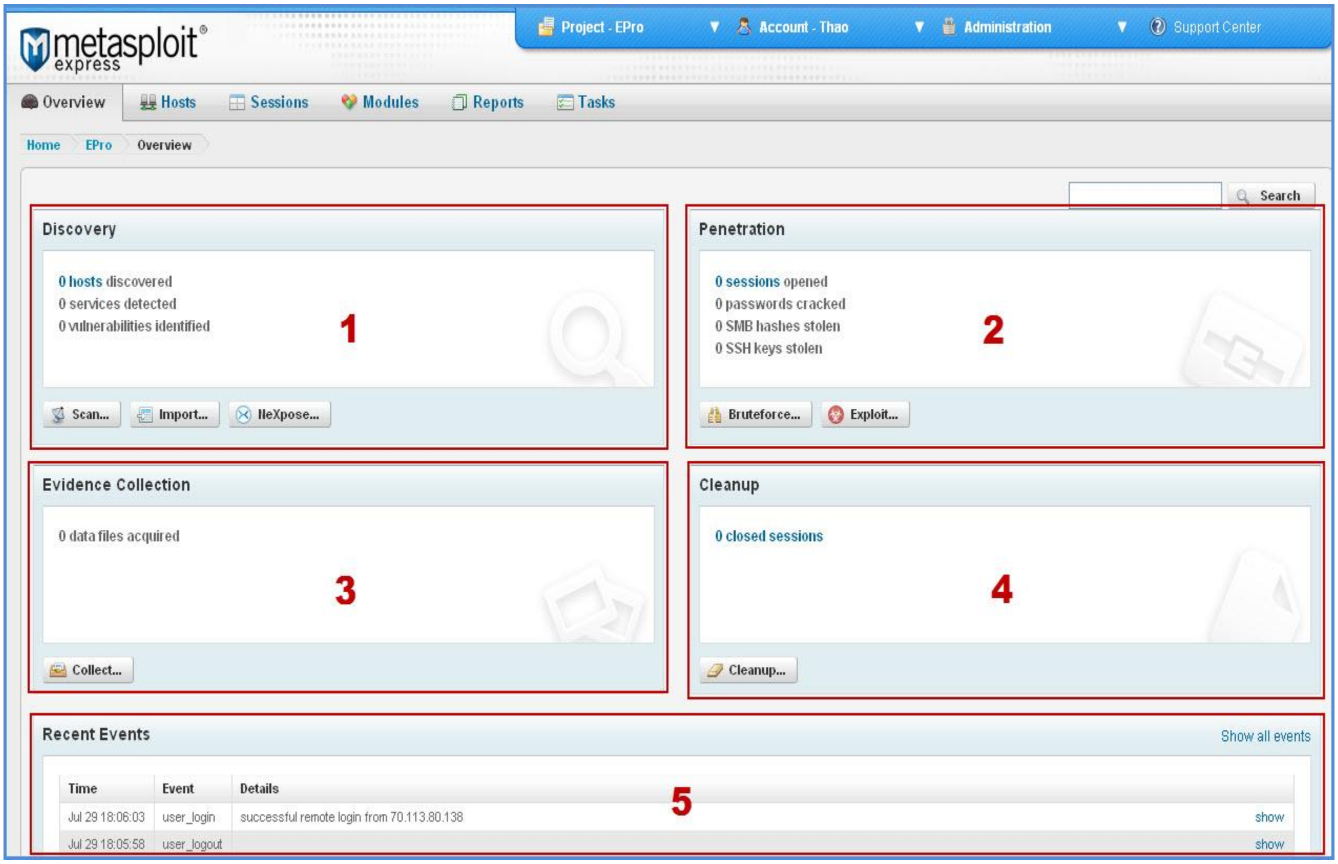
Figure 2: Projects Home Page

The **Projects** page has several notable areas:

1. **Navigational breadcrumbs** – Use the **Home** link to access the **Projects** page.
2. **Projects** – All projects are listed on the **Projects** page. Simply click on a project name to open it.
3. **Host/Session status** – Quickly view host and session statuses directly on the Projects page.
4. **Global Search** – Search for any host in any project to which you have access.
5. **New project** – All new projects are created through this page.
6. **Settings** – All project settings can be modified through this page; this includes project names, project descriptions, network ranges, and user access.
7. **Delete projects** – Easily delete any unnecessary projects directly from the **Projects** page.

Overview Page Tour

The **Overview** page for each project is a high-level view of the penetration testing progress. There are shortcuts on the **Overview** page you can use to initiate or review the basic testing stages for the project. All penetration testing stages - including discovery, penetration, WebScanning, and social engineering - can be initiated from this page.



Discovery

0 hosts discovered
0 services detected
0 vulnerabilities identified

Penetration

0 sessions opened
0 passwords cracked
0 SMB hashes stolen
0 SSH keys stolen

Evidence Collection

0 data files acquired

Cleanup

0 closed sessions

Recent Events

Time	Event	Details	
Jul 29 18:06:03	user_login	successful remote login from 70.113.80.138	show
Jul 29 18:05:58	user_logout		show

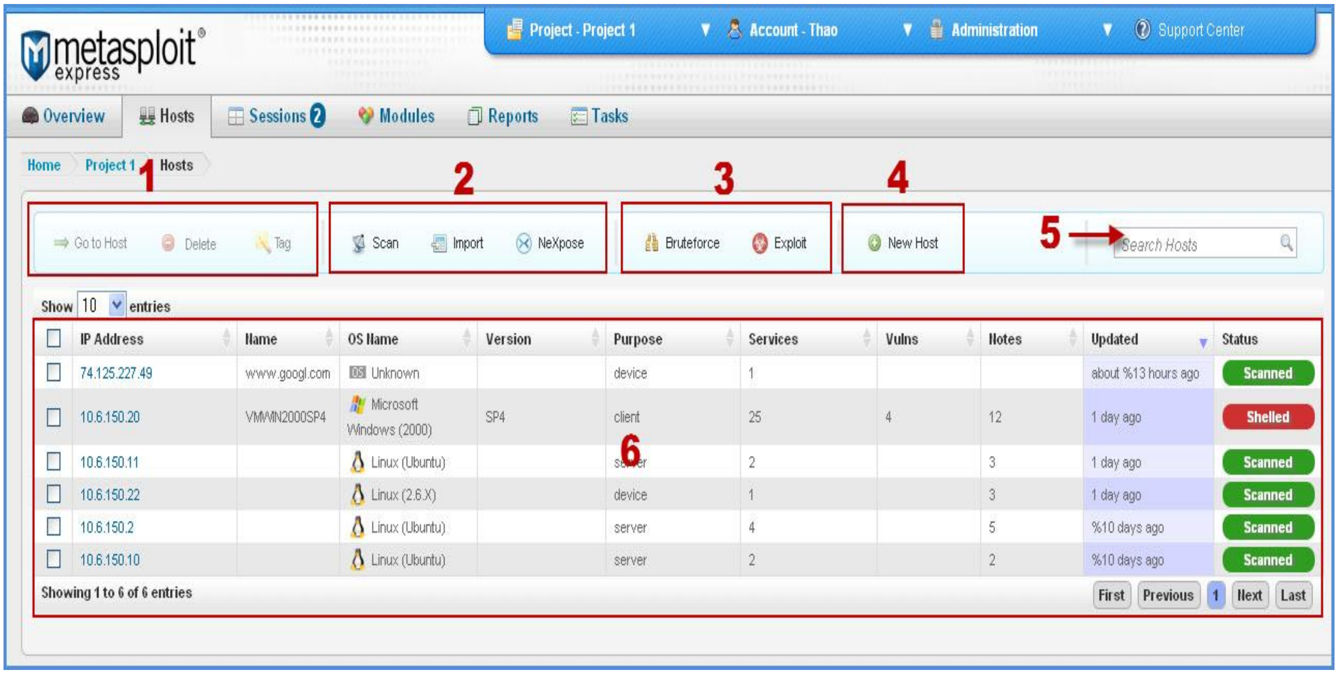
Figure 3: Overview Page

The **Overview** page includes the following notable areas:

1. **Discovery** – Run a discovery scan, data import, or NeXpose scan directly from the Discovery pane.
2. **Penetration** – Bruteforce or exploit target hosts directly from the Penetration pane.
3. **Web App** – Run a WebScan directly from the Web Apps pane.
4. **Social Engineering** – Create a new Campaign from the Web Apps pane.
5. **Recent Events** – Lists a log of recent activity on the system; use the **Show** link to view more details on the event.

Hosts Page Tour

The **Hosts** page contains a detailed, sortable list of the live hosts that were identified during the scan process.



Show 10 entries

□	IP Address	Name	OS Name	Version	Purpose	Services	Vulns	Notes	Updated	Status
□	74.125.227.49	www.googl.com	Unknown		device	1			about %13 hours ago	Scanned
□	10.6.150.20	VMWIN2000SP4	Microsoft Windows (2000)	SP4	client	25	4	12	1 day ago	Shelled
□	10.6.150.11		Linux (Ubuntu)		server	2		3	1 day ago	Scanned
□	10.6.150.22		Linux (2.6.X)		device	1		3	1 day ago	Scanned
□	10.6.150.2		Linux (Ubuntu)		server	4		5	%10 days ago	Scanned
□	10.6.150.10		Linux (Ubuntu)		server	2		2	%10 days ago	Scanned

Showing 1 to 6 of 6 entries

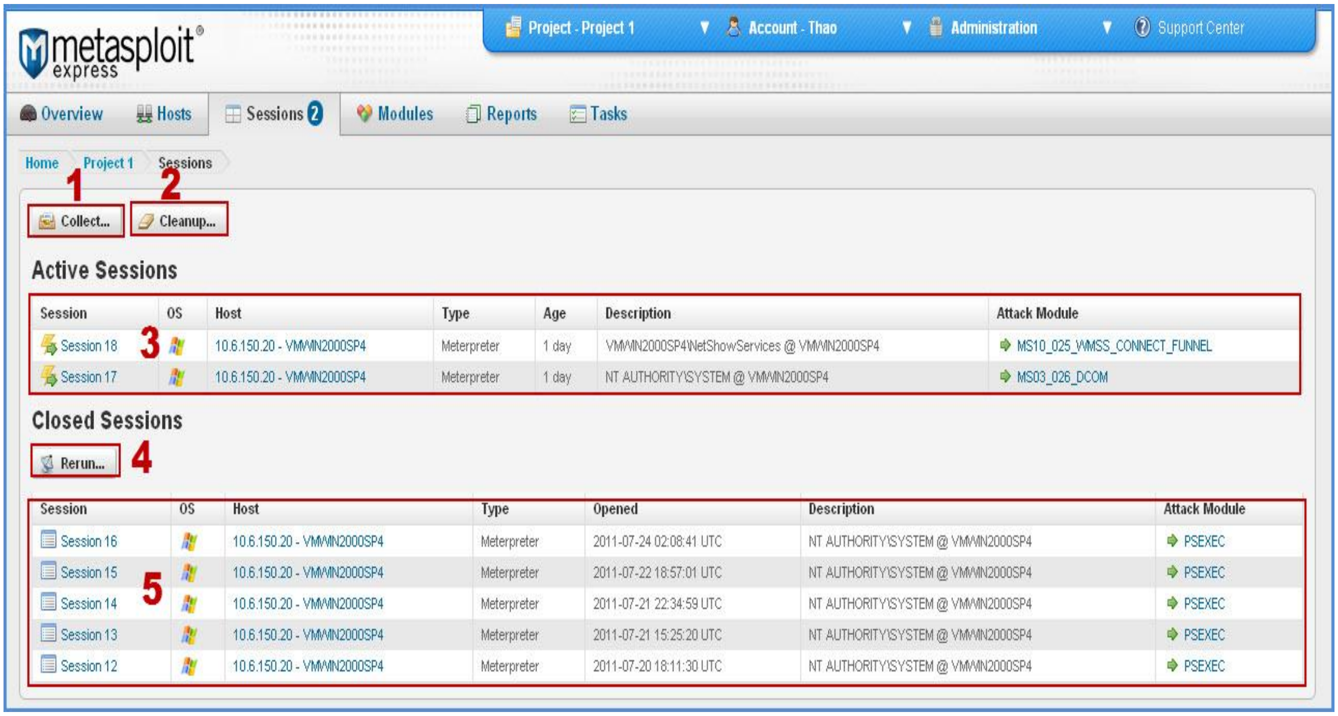
Figure 4: Hosts page

The **Hosts** page has the following notable areas:

1. **Manage hosts** – Delete and tag hosts.
2. **Run scans** – Discover hosts by running a discovery scan, NeXpose scan, Web scan, or by importing your own scan data.
3. **Exploit hosts** – Use bruteforce or automated exploits to gain access to target hosts.
4. **New hosts** – Manually add a target host.
5. **Search** – Use keywords to search for a host.
6. **Hosts** – Lists the available hosts and their information (IP address, name, version, services, vulnerabilities, tags, status).

Sessions Page Tour

The **Sessions** page lists the open and closed sessions (persistent connections) that were opened during the bruteforce or exploitation of a host. Sessions are also opened when a background module, such as a browser exploit, succeeds in exploiting a client system.



Active Sessions

Session	OS	Host	Type	Age	Description	Attack Module
Session 18		10.6.150.20 - VMWIN2000SP4	Meterpreter	1 day	VMWIN2000SP4\NetShowServices @ VMWIN2000SP4	MS10_025_WMSS_CONNECT_FUNNEL
Session 17		10.6.150.20 - VMWIN2000SP4	Meterpreter	1 day	NT AUTHORITY\SYSTEM @ VMWIN2000SP4	MS03_026_DCOM

Closed Sessions

Session	OS	Host	Type	Opened	Description	Attack Module
Session 16		10.6.150.20 - VMWIN2000SP4	Meterpreter	2011-07-24 02:08:41 UTC	NT AUTHORITY\SYSTEM @ VMWIN2000SP4	PSEXEC
Session 15		10.6.150.20 - VMWIN2000SP4	Meterpreter	2011-07-22 18:57:01 UTC	NT AUTHORITY\SYSTEM @ VMWIN2000SP4	PSEXEC
Session 14		10.6.150.20 - VMWIN2000SP4	Meterpreter	2011-07-21 22:34:59 UTC	NT AUTHORITY\SYSTEM @ VMWIN2000SP4	PSEXEC
Session 13		10.6.150.20 - VMWIN2000SP4	Meterpreter	2011-07-21 15:25:20 UTC	NT AUTHORITY\SYSTEM @ VMWIN2000SP4	PSEXEC
Session 12		10.6.150.20 - VMWIN2000SP4	Meterpreter	2011-07-20 18:11:30 UTC	NT AUTHORITY\SYSTEM @ VMWIN2000SP4	PSEXEC

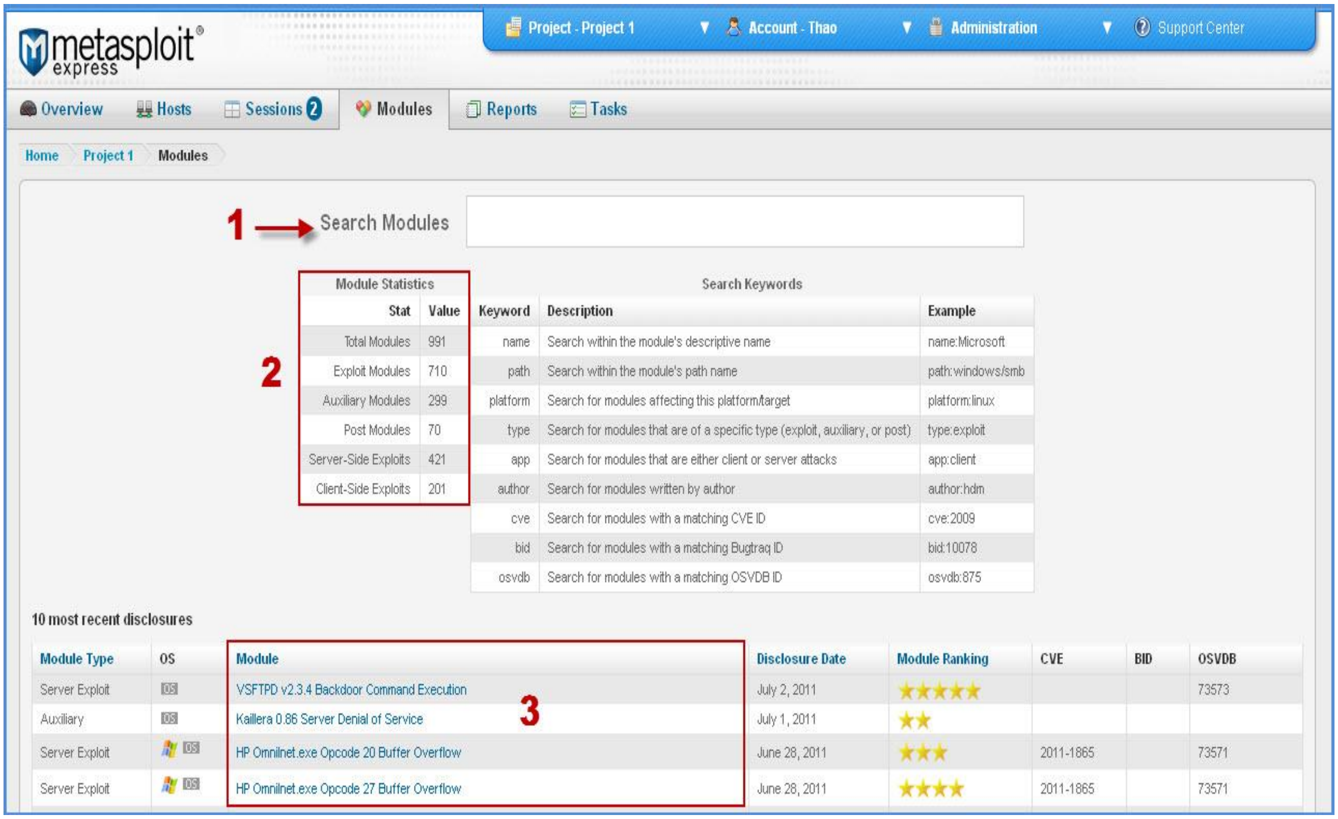
Figure 5: Sessions Page

The **Sessions** page has the following notable areas:

1. **Collect Evidence** – Collect system data from exploits on target systems.
2. **Cleanup Sessions** – Close any active sessions.
3. **Interact with Sessions** – Click on a session name to view the options for each session. These options will allow you to interact with an active session (e.g., collect system data, access file systems, create Proxy/VPN Pivots, etc.).
4. **Rerun successful attacks** – Rerun all attacks that successfully opened sessions.
5. **View Closed Sessions** – Click on a session name to see its details; this includes the even type and any session data.

Modules Page Tour

The Modules page provides a way to search, view, and execute standard auxiliary or exploit modules.



Module Statistics

Stat	Value
Total Modules	991
Exploit Modules	710
Auxiliary Modules	299
Post Modules	70
Server-Side Exploits	421
Client-Side Exploits	201

Search Keywords

Keyword	Description	Example
name	Search within the module's descriptive name	name:Microsoft
path	Search within the module's path name	path:windows/smb
platform	Search for modules affecting this platform/target	platform:linux
type	Search for modules that are of a specific type (exploit, auxiliary, or post)	type:exploit
app	Search for modules that are either client or server attacks	app:client
author	Search for modules written by author	author:hdm
cve	Search for modules with a matching CVE ID	cve:2009
bid	Search for modules with a matching Bugtraq ID	bid:10078
osvdb	Search for modules with a matching OSVDB ID	osvdb:875

10 most recent disclosures

Module Type	OS	Module	Disclosure Date	Module Ranking	CVE	BID	OSVDB
Server Exploit	OS	VSFTPD v2.3.4 Backdoor Command Execution	July 2, 2011	★★★★★			73573
Auxiliary	OS	Kaillera 0.86 Server Denial of Service	July 1, 2011	★★			
Server Exploit	OS	HP Omnilnet.exe Opcode 20 Buffer Overflow	June 28, 2011	★★★	2011-1865		73571
Server Exploit	OS	HP Omnilnet.exe Opcode 27 Buffer Overflow	June 28, 2011	★★★★	2011-1865		73571

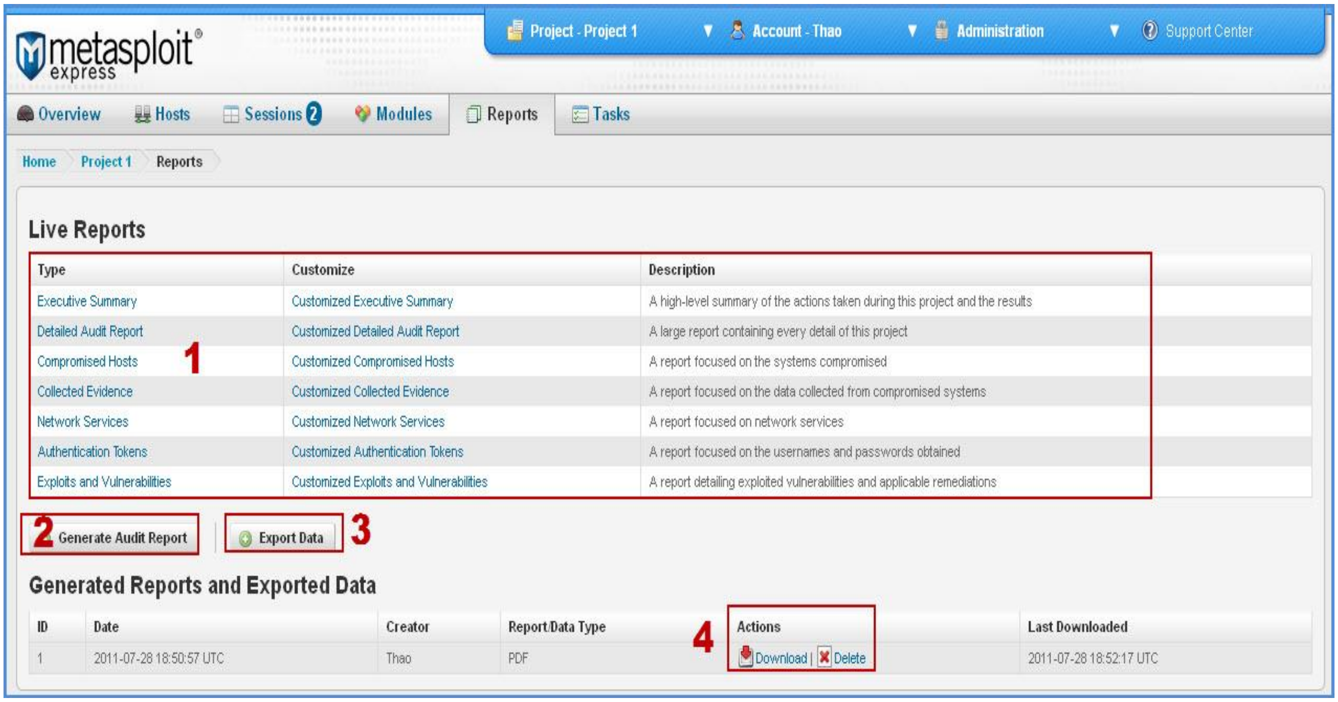
Figure 6: Modules Page

From the **Modules** page, you can perform several actions:

1. **Search for an exploit** – Run a search based on the module's name, path, platform, type, and other parameters.
2. **Look at totals** – Review statistics about the total number of modules, and the breakdown between exploit vs. auxiliary and server-side vs. client-side modules.
3. **Manually launch an exploit** – Select a module from the list of filtered module search results to configure for a manual attack.

Reports Page Tour

The Reports page provides a list of live HTML reports and generated reports. The generated reports are static reports that can be exported and saved.



Live Reports

Type	Customize	Description
Executive Summary	Customized Executive Summary	A high-level summary of the actions taken during this project and the results
Detailed Audit Report	Customized Detailed Audit Report	A large report containing every detail of this project
Compromised Hosts	Customized Compromised Hosts	A report focused on the systems compromised
Collected Evidence	Customized Collected Evidence	A report focused on the data collected from compromised systems
Network Services	Customized Network Services	A report focused on network services
Authentication Tokens	Customized Authentication Tokens	A report focused on the usernames and passwords obtained
Exploits and Vulnerabilities	Customized Exploits and Vulnerabilities	A report detailing exploited vulnerabilities and applicable remediations

Generated Reports and Exported Data

ID	Date	Creator	Report/Data Type	Actions	Last Downloaded
1	2011-07-28 18:50:57 UTC	Thao	PDF	Download | Delete	2011-07-28 18:52:17 UTC

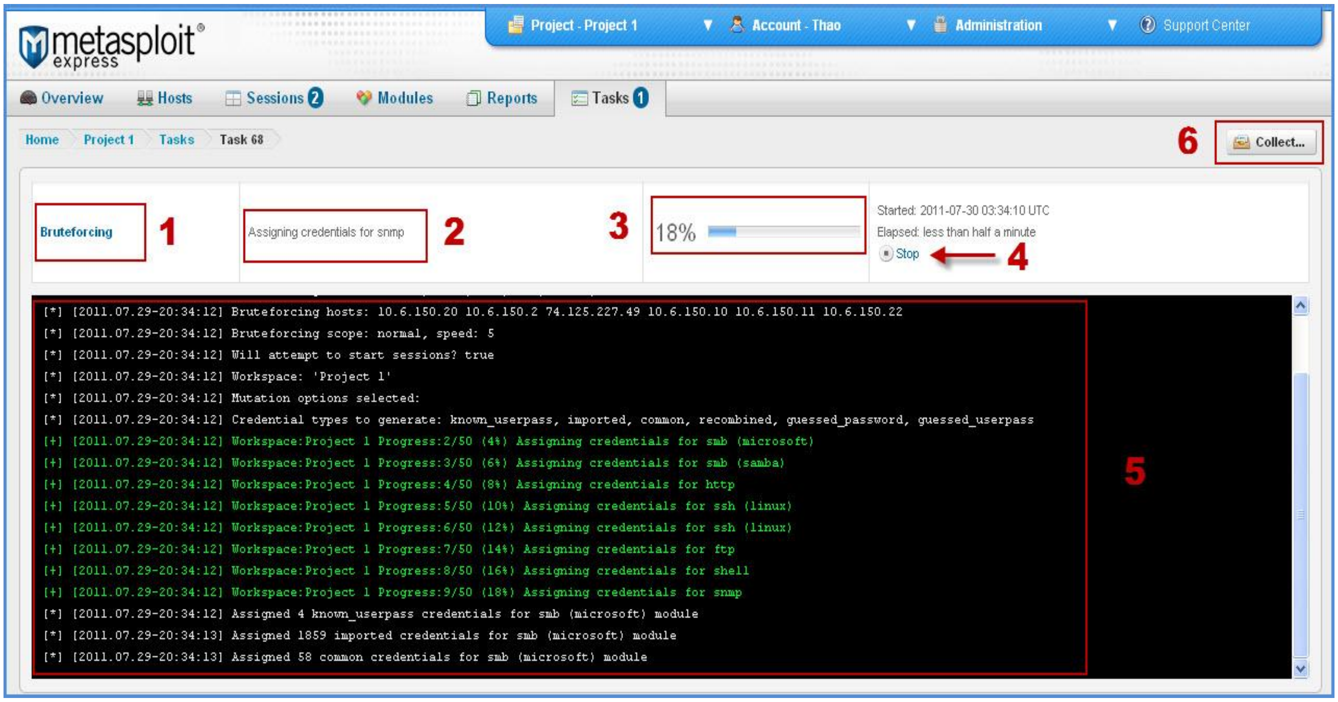
Figure 7: Reports page

From the **Reports** page, you can:

1. **View an instant report** - Click a report type from the **Live Reports** section.
2. **Create a PDF report or in another format** - Click **Generate Audit Report** and select the **PDF** option or any of the other available formats (XML, Word, ZIP, etc.).
3. **Export data from the penetration test** – Click **Export Data** to generate all the data found during the penetration test. Select whether the report will be downloadable as a PDF, XML, RTF, ZIP, PWDump, or Replay file.
4. **Download or delete existing reports** – Click the **Download** button to view an existing report or **Delete** to permanently remove a report from the system.

Task Page Tour

The **Tasks** page is a real-time log of user-initiated activities (e.g., discovery, bruteforce, exploit, and cleanup), their completion status, and the duration of completed tasks. There are essentially two Task pages: the main task page that shows a list of the completed and running tasks and the individual task page that shows the detailed progress of a task.



Bruteforcing

Assigning credentials for snmp

18%

Started: 2011-07-30 03:34:10 UTC
Elapsed: less than half a minute

```
[*] [2011.07.29-20:34:12] Bruteforcing hosts: 10.6.150.20 10.6.150.2 74.125.227.49 10.6.150.10 10.6.150.11 10.6.150.22
[*] [2011.07.29-20:34:12] Bruteforcing scope: normal, speed: 5
[*] [2011.07.29-20:34:12] Will attempt to start sessions? true
[*] [2011.07.29-20:34:12] Workspace: 'Project 1'
[*] [2011.07.29-20:34:12] Mutation options selected:
[*] [2011.07.29-20:34:12] Credential types to generate: known_userpass, imported, common, recombined, guessed_password, guessed_userpass
[+] [2011.07.29-20:34:12] Workspace:Project 1 Progress:2/50 (4%) Assigning credentials for smb (microsoft)
[+] [2011.07.29-20:34:12] Workspace:Project 1 Progress:3/50 (6%) Assigning credentials for smb (samba)
[+] [2011.07.29-20:34:12] Workspace:Project 1 Progress:4/50 (8%) Assigning credentials for http
[+] [2011.07.29-20:34:12] Workspace:Project 1 Progress:5/50 (10%) Assigning credentials for ssh (linux)
[+] [2011.07.29-20:34:12] Workspace:Project 1 Progress:6/50 (12%) Assigning credentials for ssh (linux)
[+] [2011.07.29-20:34:12] Workspace:Project 1 Progress:7/50 (14%) Assigning credentials for ftp
[+] [2011.07.29-20:34:12] Workspace:Project 1 Progress:8/50 (16%) Assigning credentials for shell
[+] [2011.07.29-20:34:12] Workspace:Project 1 Progress:9/50 (18%) Assigning credentials for snmp
[*] [2011.07.29-20:34:12] Assigned 4 known_userpass credentials for smb (microsoft) module
[*] [2011.07.29-20:34:13] Assigned 1859 imported credentials for smb (microsoft) module
[*] [2011.07.29-20:34:13] Assigned 58 common credentials for smb (microsoft) module
```

Figure 8: Individual Task Page

The **Tasks** page has several notable areas:

1. **Task** – Shows the task that Metasploit Express is currently performing.
2. **Description** – Provides a description of the action Metasploit Express is performing.
3. **Task bar** – Tracks the progress of the task.
4. **Log** – Shows the log for the running task.
5. **Stop** – Use the **Stop** button to stop the task from running.
6. **Collect** – Use the **Collect** button to gather information.

Getting Started with Metasploit Express

The following sections will provide you with information on how to get started with Metasploit Express – this includes installing the test tool and launching it for the first time.

Installing Metasploit Express

Before you get started, you must have Metasploit Express installed on your system. For more information on installing Metasploit Express, please see the *Metasploit Express Installation Guide*. The Installation Guide will provide you with the necessary instructions and information to get you up and running.

System Requirements

Before installing Metasploit Express, make sure that your system meets the minimum system requirements. See the specifications below:

2 GHz+ processor
2 GB RAM available (increase accordingly with VM targets on the same device)
500MB+ available disk space
10/100 Mbps network interface card

Operating Systems

Metasploit Express is supported on the following operating systems:

Windows XP SP2+
Windows Vista
Windows 7
Windows 2003 Server SP1+
Windows 2008 Server
RHEL 5+
Ubuntu 8.08+

Now you are ready to get started with Metasploit Express. The following sections will explain how to launch the application and how to create a user account.

Supported Browsers

Metasploit Express currently officially supports the following browsers:

- Chrome 8+
- Firefox 4+
- Internet Explorer 9+

All other browsers and versions may work, but there may be visual differences between the supported and unsupported browsers.

Virtual Appliances

Metasploit Pro is available as an Amazon EC2 cloud and VMware OVF Virtual Appliance. For more information about the virtual appliances, see:

- Amazon EC2 Virtual Appliance Quick Start Guide
- Vmware OVF Virtual Appliance Quick Start Guide

Creating a User Account

The first launch of Metasploit Express opens a browser window with a **Setup and Configuration** web form. For each installation of Metasploit Express, you can create up to three user accounts. If left unassigned, users will have regular access to Metasploit Express, which enables them to only access projects that have been authorized for them.

If a user is assigned an Administrator role, they will be able to access all projects, manage user accounts, and perform software updates. There can be multiple administrator roles assigned.

Note: To access the **User Accounts** area after the first launch, select **Administration > User Administration** from the navigational breadcrumbs located at the upper right corner of the interface. The user account creation process will be the same as the first time.

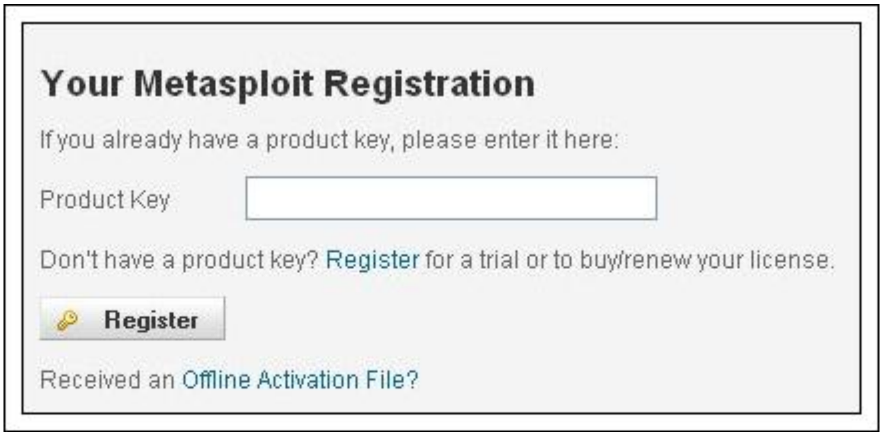
To create a new user:

1. Enter your desired username in the **Username** field.
2. Enter your first and last name in the **Full name** field.
3. Enter a strong password in the **Password** field. Strong passwords are recommended because Metasploit Express runs as root. Use mixed case, punctuation, numbers, and at least 6 characters. Re-enter the password in the Password confirmation field.
4. Re-enter your password in the **Password** confirmation field.
5. Click **Save Changes**.

Note: If you forget your password, there is a password reset script located in your Metasploit Express installation directory under $INSTALLERBASE/apps/pro/ui/script/resetpw. Once your user account has been successfully created, Metasploit Express will display the **Projects** page.

Registering the Product

After the first user account has been created, Metasploit Express will prompt you to register the product. You can enter your Metasploit Express product key (provided via email) into the **Product Key** field and click **Register**. This will verify the validity of the provided key.



Your Metasploit Registration

If you already have a product key, please enter it here:

Product Key

Don't have a product key? Register for a trial or to buy/renew your license.

Received an Offline Activation File?

Figure 9: Register Product

After a valid key has been supplied, Metasploit Express will prompt for activation. This will send your key, along with a small amount of system information to the Metasploit licensing server. A proxy can be entered at this phase, if necessary.

After a successful activation, you will be taken to the **Projects** page.

Running Metasploit Express

You can run Metasploit Express on Windows or in Linux. The following two sections detail how to launch Metasploit Express in both operating systems.

Launching Metasploit Express in Windows

To access Metasploit Express in Windows, navigate to **Start > All Programs > Metasploit**. To run the Web client, select the application **Access Metasploit Express**.

You can manually install, start, stop, and uninstall Metasploit Express services by using the options under the Metasploit Express Service subdirectory.

Launching Metasploit Express in Linux

The Linux installer places a startup script in the root directory of the install - **`$INSTALLERBASE/ctlscript.sh`**. This script can be used to start, stop, and check the status of the Metasploit services. Additionally, if you chose to install Metasploit Express as a service, a symbolic link to the ctlscript.sh script will be placed in the **`/etc/init.d`** directory.

To run the web client for Metasploit Express in Linux, browse to https://localhost:3790 (assuming the default SSL port was chosen).

Setting Up a Target (Metasploit Vulnerable VMs)

You will need to configure a target network before penetration testing can begin. Rapid7 provides vulnerable virtual machines you can install as a guest system on your local machine for testing purposes. The Metasploitable and UltimateLAMP vulnerable VMs are an Ubuntu machines running vulnerable services and containing weak accounts.

The Metasploitable VM focuses on network-layer vulnerabilities, while the UltimateLAMP VM is primarily focused on web vulnerabilities.

If you're familiar with VMWare and have a workstation or, server already installed, that can be used as a VM host. Alternatively, you can get the free VMWare Player here: http://www.vmware.com/products/player/.

The Metasploitable vulnerable VM runs the following services:

- FTP
- Secure Shell
- Telnet
- DNS
- Apache
- Postgres 8.3
- MySQL
- Tomcat 5.5
- DistCC

The Metasploitable VM also contains a weak system account with the username user and the password user. Several vulnerable applications have been installed on the VM.
The UltimateLAMP VM runs the following services:

- Postfix
- Apache
- MySQL

Additionally UltimateLAMP runs older and vulnerable versions of the following applications:

- Wordpress
- TextPattern
- Serendipity

- MediaWiki
- TikiWiki
- PHP Gallery
- Moodle
- PHPWebSite
- Joomla
- eGroupWare
- Drupal
- Php Bulletin Board
- Sugar CRM
- Owl
- WebCalendar
- Dot Project
- PhpAdsNew
- Bugzilla
- OsCommerce
- ZenCart
- PhphMyAdmin
- Webmin
- Mutillidae 1.5 (OWASP Top 10 Vulns)

The UltimateLAMP VM's default credentials are: 'root': 'vmware'. Each application is available by browsing to:80 on the VM's assigned IP address.

System Requirements for Host and Guest Systems

For a typical host system that will run Metasploit Express and VMware, we recommend a 2GHz or faster processor and a minimum of 3GB of memory.

VMware Player requires approximately 150MB of disk space to install the application on the host, and at least 1GB of disk space is recommended for each guest operating system. For more details on minimum PC requirements, see the VMware Player Documentation.

You must have enough memory to run the host operating system, in addition to the memory required for each guest operating system and the memory required for Metasploit Express. Please see your guest operating system and application documentation for their memory requirements.

The vulnerable VM requires VMWare 6.5 or above and approximately 1.5GB of disk space to run properly.

Obtaining the Vulnerable VM

To access and download the UltimateLAMP and Metasploitable VMs, visit http://www.metasploit.com/community/ for the public BitTorrent link. An HTTP download is available from within the customer portal. An up-to-date README file is also available with the VMs.

Setting Up the Vulnerable VM

You will need to download and install the vulnerable VM in your local machine as a guest system. The virtual device is approximately 600MB and will take about 10 minutes to download on a modern cable connection.

Once the VM is available on your desktop, open the device and run with VMWare Player. Alternatively, you can also use VMWare Workstation or VMWare Server.

Once you have a vulnerable machine ready, it's time to begin your penetration test on Metasploit Express. You will need to log into your Metasploit Express account to get started.

Common Vulnerabilities and Exposures (CVE)

The following sections describe to use CVE references within the Metasploit Express product.

Module Browser

The Module Browser within Metasploit Express provides specific support for CVE references. To search for an exploit or auxiliary module by its CVE reference, simple enter "CVE:IDENTIFIER" into the search form. One example of this would be: "CVE:2008-4250" to locate the Microsoft Server Service Relative Path Stack Corruption exploit.

Host Vulnerabilities

After successfully compromising a target system with the product, the Vulns tab of the Host screen will be updated to reflect what vulnerabilities were exploited. These vulnerabilities will display their corresponding CVE references.

Reporting

The Detailed Audit Report, Exploited Vulnerabilities Report, and Generated Reports (PDF) will each include references to any application CVE identifiers, as they relate to vulnerabilities found on the tested network.

About CVE

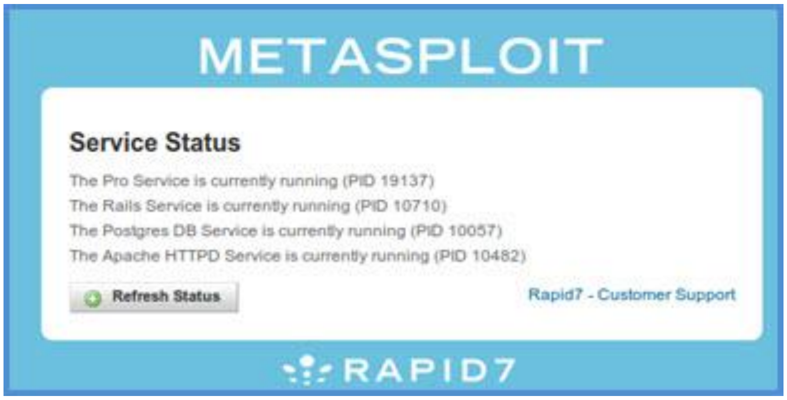
Common Vulnerabilities and Exposures (CVE®) is a dictionary of common names (i.e., CVE Identifiers) for publicly known information security vulnerabilities, while its Common Configuration Enumeration (CCE™) provides identifiers for security configuration issues and exposures.

CVE’s common identifiers make it easier to share data across separate network security databases and tools, and provide a baseline for evaluating the coverage of an organization’s security tools. If a report from one of your security tools incorporates CVE Identifiers, you may then quickly and accurately access fix information in one or more separate CVE-compatible databases to remediate the problem.

Error Recovery

Error Recovery will occur in any case where Metasploit Express crashes or is unavailable.

A watchdog process is launched at Metasploit startup and will monitor for unexpected shutdown of any of the four Metasploit services. If a service is determined to be unavailable and improperly shut down, it will be restarted automatically. Normal service stop/start actions can still be performed with start menu shortcuts (on Windows) and startup scripts (on Linux).



Service Status

The Pro Service is currently running (PID 19137)
The Rails Service is currently running (PID 10710)
The Postgres DB Service is currently running (PID 10057)
The Apache HTTPD Service is currently running (PID 10482)

Figure 10: Service Status

Administration

The following sections will provide information on the administrative tasks available in Metasploit Express.

User Accounts

Each installation of Metasploit Express allows one user account. This account should have been created when you launched Metasploit Express for the first time.

Editing a User Account

User account settings can be edited/update at any time. This includes updating the user name, email address, and time zone. Additionally, you can change your password on the **User Settings** page.

To edit a user account:

1. Select **Account > User Settings** from the Main menu.
2. Edit any of the following fields:
   - Full Name
   - Email
   - Organization
   - Time Zone
3. Click the **Save Settings** button.

Changing the Password for Your User Account

User account passwords can be changed on the **User Settings** page. Remember that passwords must pass all the strength requirements before it is accepted. These requirements include:

- Six character minimum
- Cannot contain the username
- Cannot be a common password or predictable sequence of characters.

To change the password for your user account:

1. Select **Account > User Settings** from the Main menu.
2. Enter a new password in the **New Password** field.
3. Re-enter the new password in the **New Password Confirmation** field.
4. Click the **Change Password** button.

Updating License Keys

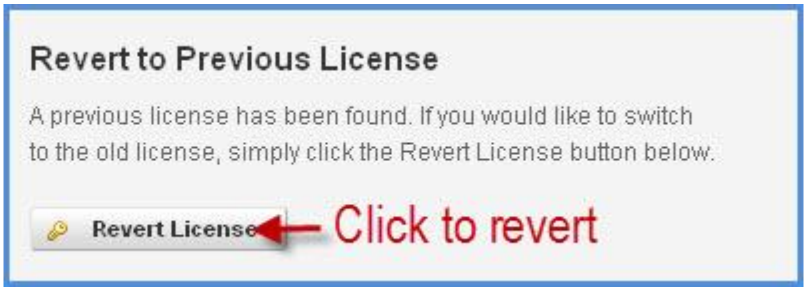
You can update your license key from the Software Updates area of the interface.

To update a license key:

1. Select **Administration > Software Updates** from the Main menu.
2. Click the **Change Key** link located under the **License Details** area.
3. Enter in the new key in the **Product Key** field.
4. Click the **Register** button.
5. Click the **Activate** button to activate your key.

Reverting to a Previous License Key

Metasploit Express will allow you to revert to previous license keys if it detects that there is one available.



Revert to Previous License

A previous license has been found. If you would like to switch to the old license, simply click the Revert License button below.

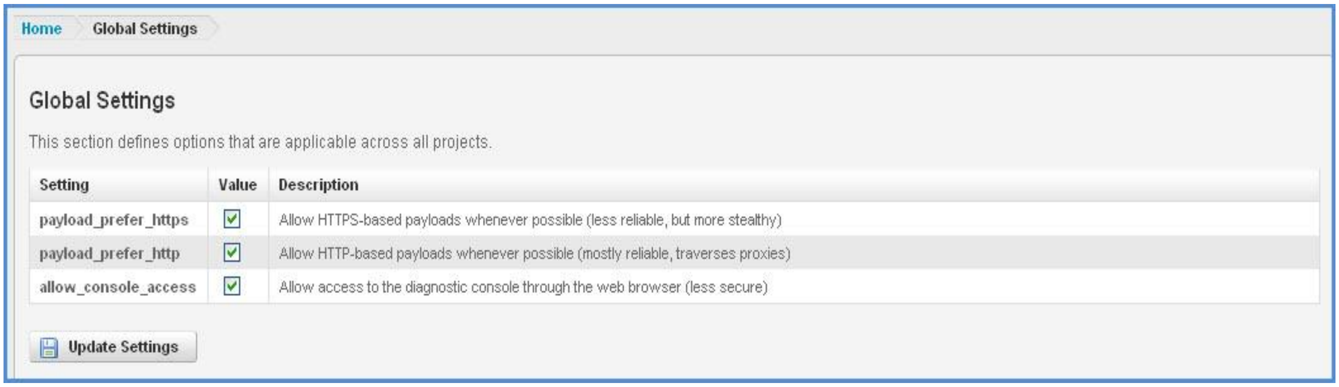
Figure 11: Revert to a previous license

To revert to a previous license key:

1. Select **Administration > Software Updates** from the Main menu.
2. Click the **Change Key** link.
3. Click the Revert License button. A new window will display alerting you if the reversion has been successful.

Configuring Global Settings

Global settings are applied across all projects. These settings enable you to set HTTP and HTTPS based payloads for all projects as well as enable you to access diagnostic console via Web browser.



Global Settings

This section defines options that are applicable across all projects.

Setting	Value	Description
payload_prefer_https	☑	Allow HTTPS-based payloads whenever possible (less reliable, but more stealthy)
payload_prefer_http	☑	Allow HTTP-based payloads whenever possible (mostly reliable, traverses proxies)
allow_console_access	☑	Allow access to the diagnostic console through the web browser (less secure)

Figure 12: Global Settings

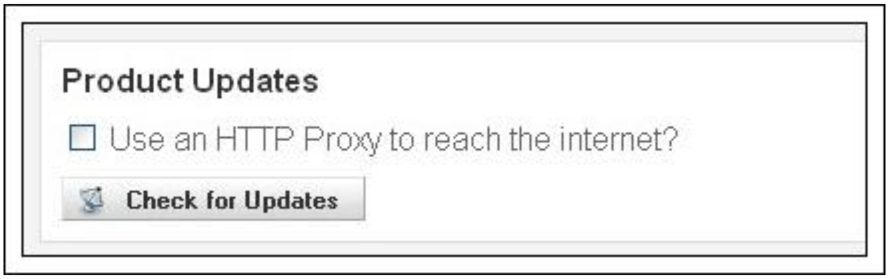
To set global options:

1. Select **Administration > Global Settings** from the Main menu.
2. Select/Deselect any of the following settings:
   - Payload_prefer_https – Allows HTTPS-based payloads whenever possible.
   - Payload_prefer_http – Allows HTTP-based payloads whenever possible.
   - Payload_prefer_access – Allows access to the diagnostic console through the Web browser.
3. Click **Update Settings**.

Updating Metasploit Express

You can check for product updates by selecting **Administration > Software Updates** located in the upper-right corner of the interface.

This will take you to the **Software Updates** page, which will display the license and registration information for your version of Metasploit Express. The **Check for Updates** button located under the **Product Updates** area enables you to manually check for product updates. If you want to use an HTTP Proxy server, then select the **Use an HTTP Proxy to reach the internet** option before clicking the **Check for Updates** button. Once the proxy option is selected, configurable proxy settings will display. Enter the information for HTTP proxy you wish to use in the appropriate fields.


Product Updates

□ Use an HTTP Proxy to reach the internet?

Figure 13: Product updates

If an update is available, the application will list the available version. Click on the **Install** button to install the latest update of Metasploit Express.

If there are no current updates, you will receive a notification that you are using the latest version.

Note: After the update has completed, a button will appear for restarting the backend services. Restarting these services will terminate any active sessions and will require up to 5 minutes before the product is usable.

Maintaining Metasploit Express

The following sections describe how to maintain Metasploit Express on Linux and Windows. Metasploit Express uses the following files to log information:

- `$INSTALL_ROOT/postgres/postgresql.log – Database log`
- `$INSTALL_ROOT/apache2/logs/error_log – Web server error log`
- `$INSTALL_ROOT/apache2/logs/access_log – Web server access log`
- `$INSTALL_ROOT/apps/pro/ui/log/production.log – Rails (ruby) log`
- `$INSTALL_ROOT/apps/pro/ui/log/thin.log - Rails (server) log`
- `$INSTALL_ROOT/apps/pro/engine/config/logs/framework.log – Metasploit Framework log`
- `$INSTALL_ROOT/apps/pro/engine/prosvc.log – Metasploit RPC log`
- `$INSTALL_ROOT/apps/pro/engine/tasks – Task logs (for individual tasks such as discover, bruteforce, etc)`
- `$INSTALL_ROOT/apps/pro/engine/license.log – License log`

Note: There is currently no automatic rotation for these logs, and over time, the various logs will grow to be very large. If disk space is an issue, please review these files regularly (at least monthly).

Uninstalling Metasploit Express

The following sections describe how to uninstall Metasploit Express on Linux and Windows.

Linux (RHEL / Ubuntu)

To uninstall Metasploit Express from your Linux (RHEL/Ubuntu) system:

1. Stop all Metasploit services by navigating to the root of the installed directory (default: /opt/metasploit-3.7.1) and typing `./ctlscript.sh stop`.
2. From the root of the installed directory, enter the `command. /uninstall`.

3. Click **Yes** when you are asked if you want to uninstall Metasploit Express and all of its modules.
4. Click **Yes** if you wish to delete all saved data from the penetration tests. Otherwise, click No, which will leave the **`entire $INSTALLERBASE/apps`** directory intact. All Metasploit Express data can be found in this directory.

Metasploit will then begin to remove all components of the software. This will take a few minutes. When the uninstall is complete, click **Finish**.

Windows

To uninstall Metasploit Express from your Windows machine:

1. Navigate to **Start > All Programs > Metasploit** and select **Uninstall Metasploit**.
2. Click **Yes** if you wish to delete all saved data from the penetration tests. Otherwise, click **No**, which will leave the entire /apps directory intact. All Express data can be found in this directory.

Metasploit will then begin to shut down its services and remove all components of the software. This will take a few minutes. When it has completed, click **Finish**.

Metasploit Express Tasks

The following sections are divided into the most common tasks performed in Metasploit Express. For a general idea of the tasks involved in penetration testing, refer to the *Metasploit Workflow* section. It will provide a high-level overview of the tasks you are most likely to perform routinely during your penetration tests.

Metasploit Express Workflow

Penetration testing with Metasploit Express can be broken down into these general tasks:

1. Creating a project
2. Discovering devices
3. Gaining access to hosts
4. Taking control of sessions
5. Collecting evidence from target hosts
6. Cleaning up sessions
7. Generating reports

Working with Projects

The first step is to create a project, which is a container for a set of targets and the tasks involved in testing them. Projects provide a way to organize your penetration test.

A Metasploit Express project consists of a name and network boundaries (optional). Network boundaries help you set and maintain scope, which prevent you from targeting devices outside of the range of intended devices and provide a default range for tasks.

Projects can be created when testing different networks or different components of one network. For example, when doing an internal and external penetration test, you may want to create separate projects for each test. This allows you to have separate reports for each test scenario and enables you to perform comparisons between the test results.

Creating a Project

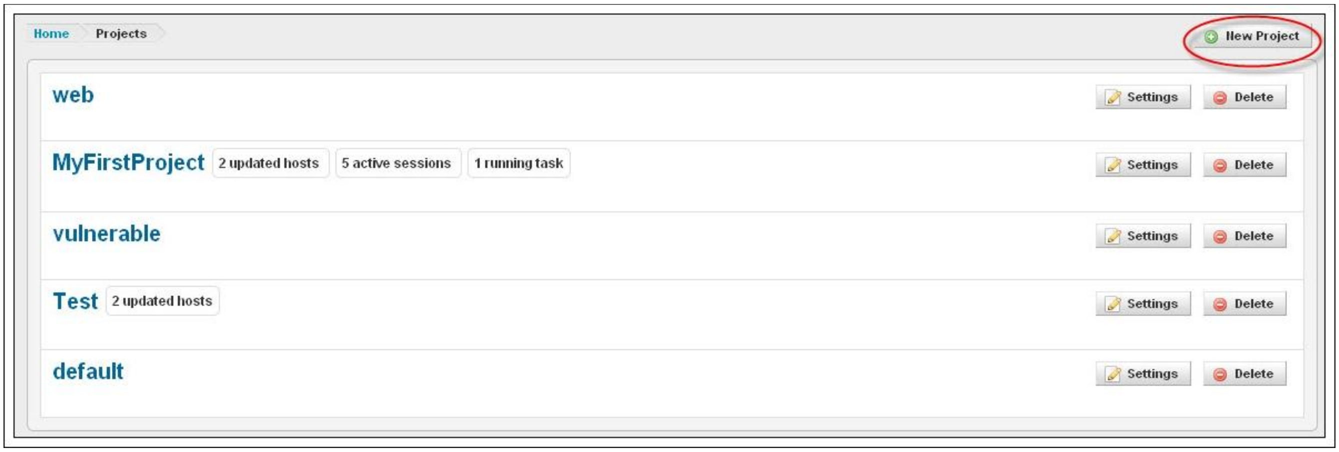


Figure 14: Creating a new Project

To create a new Project:

1. Select **Project > New Project** from the Main menu.
2. Fill in the following fields:

   - **Project Name** – This can be any name. You can change it later using the **Settings** button located on the **Projects** list page.
   - **Network Range** – These are the IP addresses that should be used as the defaults for all new tasks.
   - **Description** – Provide a description for the project.

3. Enable Restrict to Network Range if you want to enforce network boundaries on the project. If the target addresses do not fall within the project's network range, then no tasks can run.
4. Click the **Create Project** button.

Your new project will be added to the bottom of the **Projects** list. To open the project, click on the project name.

Editing Projects

To edit a Project:

1. Click on the **Home** link (located in the navigational breadcrumbs) to access the **Projects** page.
2. Click the **Settings** button for the project you would like to edit.
3. Edit any of the following **Project Settings**:

- Project Name
- Network Range Description

4. Edit any of the **User Access** settings:
    - Project Owner
    - Project Members
5. Click the **Save** button.

Viewing All Projects

To view all projects:

1. Select **Project > Show All Projects** from the Main menu.

Setting Network Boundaries

Network boundaries allow an administrator to lock tasks to a specific range, defined in the project options. The tasks that support this option are discovery, bruteforce, exploitation and reporting.

To restrict the network range for a project:

1. Open the project.
2. Select **Project > Project Settings** from the Main menu.
3. Select the **Restrict to Network Range** option.
4. Click the **Save** button.

Discovering Hosts

The first step in penetration testing is host discovery. Discovery is the Metasploit Express term for querying network services in an attempt to identify and fingerprint valid hosts. It enables Metasploit Express to determine the details of all the hosts in a target address range and enumerate the listening ports. Please note that you are responsible for supplying Metasploit Express with a valid target address range.

A number of customizable options are available for importing scan information from other tools. The scan settings are covered in further details in the *Task Settings* chapter. Additionally, Rapid7's NeXpose can be used directly from within the product to perform vulnerability scanning.

Discovering Hosts with a Scan

To perform a host discovery scan:

1. Select a project from the **Projects** list. This will open the project's **Overview** page. (Note: You can also access the **Scan** button from the **Host** page).
2. Click the **Scan** button in the Discovery pane. A **New Discovery Scan** window will open.
3. Enter the IP addresses (or address ranges) you want to target in the **Target Addresses** field.
4. Click the **Show Advanced Options** to continue configuring the scan. If no additional settings are needed, skip to the last step.
5. Enter the IP addresses (or address ranges) you want to exclude in the **Excluded Addresses** field.
6. Enter **Custom Nmap arguments**, which will take precedence over any internal configuration.
7. Click the **Portscan Speed** dropdown button to select the scan's level of stealth and essentially the scan duration.

   - **Insane** should only be used on a fast LAN.
   - **Aggressive** works well for scans across most LANs.
   - **Normal** is recommended for external use.
   - **Polite** is useful across slow WAN links or to hide the scan.
   - **Sneaky** is very stealthy but requires some time.
   - **Paranoid** requires the most amount of time to complete.

8. Enter the **Portscan Timeout** in minutes. This is a per-host timeout that is passed to Nmap.
9. Select whether to run **UDP Services Discovery**.
10. Select whether you want to **Enumerate users via Finger**.
11. Select whether you want **Identify Unknown Services** enabled.
12. Select **Single Scan** to scan each host individually.
13. Select **Dry Run** to determine what the scan will do without actually running the scan.
14. Optionally, you can set **Additional TCP Ports**, **Excluded TCP Ports**, and **Custom TCP Port Ranges, and Custom TCP Source Ports** to scan outside the default ports typically used in vulnerability scanning. The **Custom ports** option will ignore the standard ports scanned by Metasploit Express and scan just the port range entered. You can also enter an **SMB Username**, **SMB Password**, and **SMB Domain**; this information will be used by Metasploit Express with SMB username and share discovery across the network.
15. Click **Scan**.

After a scan is initiated, a **Task** page with a real-time log with a progress bar of the scanning process will open in the Metasploit Express interface. This task will be classified as “Discovering”. Leaving this page will not interrupt the scanning process. If you leave and want to review the scanning task log later, you can click the **Tasks** tab for this project and click on the task number.

When the scan is complete, you can click the project name in the page breadcrumbs to go back to the **Overview** page, where the total number of hosts discovered during the scan will be revealed in the Discovery pane.

Note: If a bruteforce is kicked off before the scan task has finished normalizing data, you may experience inaccurate results. It is suggested that you always allow scans to finish completely before performing additional actions on the hosts.

Discovering Hosts with NeXpose

Rapid7’s NeXpose (Community and Enterprise Editions) can also be used to discover and scan devices. Metasploit Express provides a simple connector that allows you to run and automatically import the results of a NeXpose scan using the Pro interface.

Before you can run a NeXpose scan, you must download, install, and configure NeXpose. Additionally, you must have configured a NeXpose server through Metasploit Express. To do this, see the section Configuring NeXpose Consoles.

- The Community Edition version of NeXpose can be downloaded from http://www.rapid7.com/vulnerability-scanner.jsp.
- Find more information on installing and configuring NeXpose at http://community.rapid7.com.
- Access the latest version of the NeXpose Installation Guide at: http://community.rapid7.com/redmine/projects/nexpose/wiki/Install_Guide.

Note: Metasploit Express currently only supports scanning the number of hosts that are licensed in NeXpose; if you supply more than your licensed number of hosts (32 in Community), the scan will fail.

To run a NeXpose scan:

1. Select a project from the **Projects** list. This will open the project’s **Overview** page. (Note: You can also access the **NeXpose** button from the **Host** page).
2. Click the **NeXpose** button located in the **Discovery** pane.
3. Select a **NeXpose console**. This list will only be populated if you have preconfigured a NeXpose server to use. This can be done from the Global Settings area of Metasploit Express. For more information on configuring NeXpose consoles, see the section Configuring NeXpose Consoles.
4. Enter the target address range in the **NeXpose Scan Targets** field.

5. Select a **Scan Template**; this is the template that will be used to scan the network. Only predefined templates are supported.

    - **Penetration Test Audit** – Performs an in-depth penetration test of all systems using only safe checks. Host-discovery and network penetration options will be enabled, allowing NeXpose to dynamically discover additional systems in your network to target. In-depth patch and hotfix checking, policy compliance checking, and application-layer auditing will not be performed.
    - **Full Audit** – Performs a full network audit of all systems using only safe checks, including network-based vulnerabilities, patch/hotfix checking, and application-layer auditing. Only default ports are scanned, and policy checking is disabled, making this faster than the Exhaustive scan.
    - **Exhaustive** – Performs an exhaustive network audit of all systems and services using only safe checks, including patch/hotfix checking, policy compliance checking, and application-layer auditing. Performing an exhaustive audit could take several hours or even days to complete, depending on the number of hosts selected.
    - **Discovery** – Performs a discovery scan to identify live devices on the network, including host name and operating system. No further enumeration, policy or vulnerability scanning will be performed.
    - **Aggressive Discovery** – Performs a fast and cursory discovery scan to identify live devices on high speed networks, including host name and operating system. Packets are sent at a very high rate which may trigger IPS/IDS sensors, SYN flood protection and exhaust states on stateful firewalls. No further enumeration, policy or vulnerability scanning will be performed.
    - **DoS Audit** – Performs a basic network audit of all systems using both safe and unsafe (denial-of-service) checks. In-depth patch/hotfix checking, policy compliance checking, and application-layer auditing will not be performed.

6. Click the **Advanced Options** button to continue configuring the scan. If no additional settings are needed, skip to the last step.
7. Select whether to **Purge the scan results** from the NeXpose Server.
8. Enable the **Specify additional scan credentials** for additional credentials to use during the scan. Enter the **Scan Credentials** that will be used to scan the hosts. This information is optional. Please note that multiple credentials are not supported; you will need to use NeXpose directly for multiple credential support.

    - **Type** – Select Windows/CIFS, Secure Shell/SSH, Telnet, HTTP, FTP, SNMP, or POP3.
    - **User** – The username used for the scan credentials.
    - **Password** – The password used for the scan credentials.

9. Click the **Launch NeXpose** button.

Configuring NeXpose Consoles

Any preconfigured NeXpose engine can be managed globally with Metasploit Express. These will act as persistent connections and can be used to import individual sites into a project.

Once you have set up your NeXpose consoles, you will be able to access them for any NeXpose scan. These consoles will be automatically available for you to choose from the **NeXpose Scan** page.

To configure a NeXpose console:

1. Select **Administration > Global Settings** from the Main menu.
2. Scroll down to **NeXpose Consoles**.
3. Click the **Configure a NeXpose Console** button.
4. Enter a **Console Name**.
5. Enter the **Console Address**.
6. Enter the **Console Port**.
7. Enter the **Console Username**.
8. Enter the **Console Password**.
9. Select **Enabled** to enable the console.

Importing Scan Data

Completed scans can be imported directly into Metasploit Express. When you import scans, the following information will be imported: hosts, ports, and services. In the case of the vulnerability scanners, additional vulnerability information will be imported.

The formats include:

- Metasploit PWDump Export
- Metasploit XML (all versions)
- Metasploit ZIP (all versions)
- NeXpose Simple XML (i.e., “XML”)
- NeXpose Raw XML (i.e., “XML Export”)
- Foundstone Network Inventory XML
- Microsoft MBSA SecScan XML
- nCircle IP360 (XMLv3 and ASPL)
- NetSparker XML
- Nessus NBE
- Nessus XML (v1 and v2)

- Qualys Asset XML
- Qualys Scan XML
- Burp Session XML
- Acunetix XML
- AppScan XML
- Nmap XML
- Retina XML
- NetSparker XML
- Amap Log
- IP Address

Note: Raw XML is only available in commercial editions of NeXpose and includes much more vulnerability information. Use this format when it is available.

To import data into a project:

1. Go to the **Overview** page.
2. Click on the **Import** button located under the **Discovery** pane of the **Overview** page. The **Import Data** window will display.
3. Click the **Browse** button to navigate to and choose the import file. Click the **Open** button after you have selected the file.
4. Enter any target addresses to be excluded in the **Exclude Addresses** field.
5. Select **Do not change existing hosts** if you do not want the information in the imported file to affect an existing host.
6. Click **Import Data** to complete the import process.

Manually Managing Vulnerabilities

The discovery process enables Metasploit Express to identify and fingerprint hosts as well as determine the details of the hosts in a target address range. During the scan, any known vulnerabilities for a target host will be identified.

If certain known vulnerabilities are not identified with the host, you can manually add the vulnerability to the target host.

Note: Before modifying any vulnerabilities, you must run a discovery scan for your project.

Adding a Known Vulnerability

To add a vulnerability to a host:

1. Click on the **Host** tab.
2. Click on a **Host** (from the IP address list).

3. Click on the **Vulnerabilities** tab.
4. Click the **New Vuln** button.
5. Enter the vulnerability's name in the **Name** field (e.g., exploit/windows/smb/psexec).
6. Enter the vulnerability's reference information (CVE identifier, OSVDB ID, etc.). Use the **Add Reference** button to add a new line of information.
7. Click the **Save** button when done.

Deleting an Identified Vulnerability

To delete a vulnerability from a host:

1. Click on the **Host** tab.
2. Click on a **Host** (from the IP address list).
3. Click on the Vulnerabilities tab.
4. Locate the vulnerability you want to delete and click the delete button.

Editing an Identified Vulnerability

To modify a vulnerability:

1. Click on the **Host** tab.
2. Click on a **Host** (from the IP address list).
3. Click on the **Vulnerabilities** tab.
4. Locate the vulnerability you want to edit and click the **edit** button.
5. Make any modifications to the vulnerability's settings and/or reference information.
6. Click **Save** to apply the changes.

Manually Adding Hosts

To manually add a host:

1. Select a project from the **Projects** list. This will open the project's **Overview** page.
2. Click the **Hosts** tab. This will open the **Hosts** page.
3. Click the **New Host** button.
4. Enter in the following information:

   - **Name** – The host name
   - **IP Address** – The host IP address
   - **Ethernet Address** – The host Ethernet address
   - **OS Name** – OS System for the host (e.g., Microsoft Windows XP, Linux)
   - **OS Version** – OS Version for the host (e.g., SP2, 2.6.x)
   - **Purpose** – Client or server

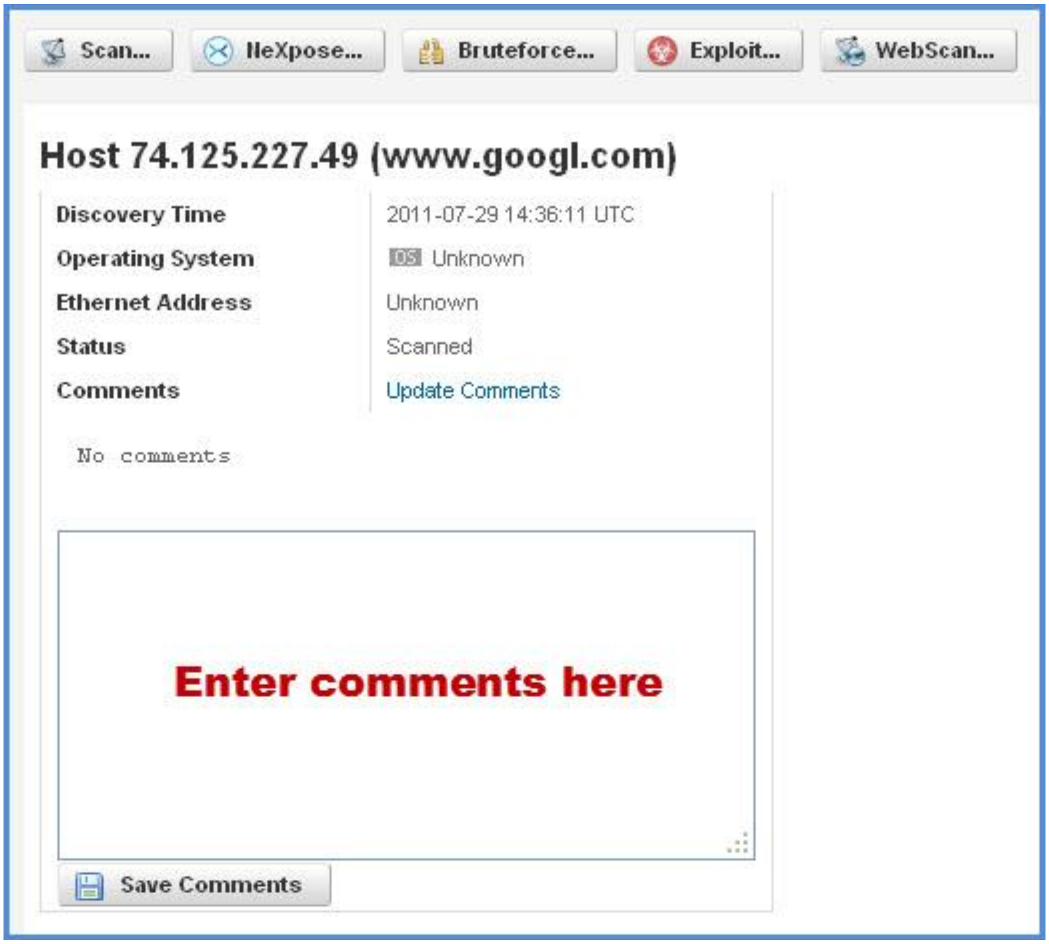
5. Click the **Add Service** link to add a service.
6. Enter the following information for the service:

- **Name** – The service name
- **Port** – The port the service runs on
- **Protocol** – The protocol for the service
- **State** – The status of the port

7. Click the **Save** button.

Host Comments

Host comments enable you to provide detailed descriptions or additional information about a particular host.



Host 74.125.227.49 (www.googl.com)

Discovery Time	2011-07-29 14:36:11 UTC
Operating System	OS Unknown
Ethernet Address	Unknown
Status	Scanned
Comments	Update Comments

No comments

Enter comments here

Figure 15: Host Commenting

To add a comment to a host:

1. Click the **Hosts** tab.
2. Click on the **IP address** of the host you would like to comment on. The host's details page will open.
3. Click on the **Update Comments** link.
4. Enter your comments in the **Comments** field.
5. Click the **Save** button.

Gaining Access to Hosts

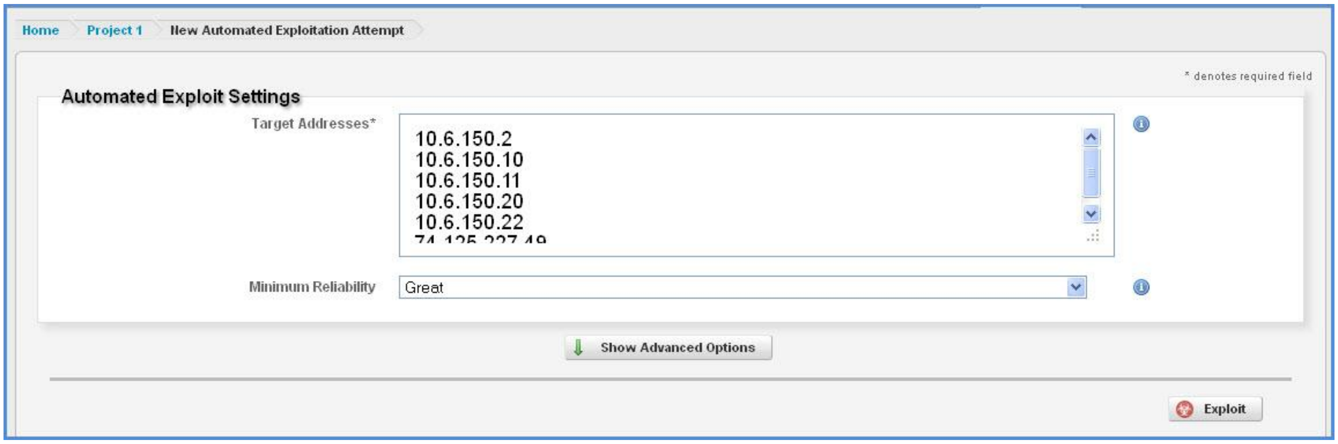
There are a few ways in which you can gain access to discovered hosts:

- Automated exploitation
- Bruteforcing
- Manual exploitation

Automated Exploitation

Exploits leverage known vulnerabilities on a device. They are distinct from the bruteforce modules because they utilize a payload (reverse connect or bind listener) and do not abuse normal authenticated control mechanisms.

The exploit feature of the Metasploit Express product cross-references open ports, imported vulnerabilities, and fingerprint information with Metasploit exploit modules.



* denotes required field

Automated Exploit Settings

Target Addresses*

10.6.150.2
10.6.150.10
10.6.150.11
10.6.150.20
10.6.150.22
74.125.227.49

Minimum Reliability: Great

Figure 16: Automated exploits

To automatically run exploits:

1. Select a project from the **Projects** list. This will open the project's **Overview** page. (You can run the automated exploit from the **Overview** page; however, this will run exploits on all hosts. From the **Host** page, you can select the hosts to run exploits against.)
2. Click the **Hosts** tab. This will open the **Hosts** page. If you have not run a discovery scan yet, you should do so at this time.
3. Select the hosts you would like to exploit. Use the **Toggle** button to select or deselect all hosts.
4. Click the **Exploit** button.
5. Under **Automated Exploit Settings**:
   - Edit the **Target Addresses** list by adding or removing any target addresses. The **Target Addresses** field will be populated with the hosts found in the last scan.
   - Click the **Minimum Reliability** dropdown button to select the reliability of the exploits you want to run:
     - **Excellent** – Exploits will never crash the service. Exploits with this ranking include SQL Injection, CMD execution, and certain weak service configurations. Most web application flaws fall into this category.
     - **Great** – Exploits will have a default target and either auto-detect the appropriate target, or use an application-specific return address after running a version check. These exploits can crash the target, but are considered the mostly likely to succeed.
     - **Good** – Exploits have a default target and it is the "common case" for this type of software (English, Windows XP for a desktop app, 2003 for server, etc.).
     - **Normal** – Exploits are reliable, but depend on a specific version and cannot reliably auto-detect.
     - **Average**– Ranked exploits are difficult to reliably leverage against some systems.
     - **Low** – The exploit fails more than 50% of the time for common platforms.
6. Click the **Advanced Options** button if there are additional settings you want to configure. If not, then skip to the last step.
7. Under **Targeting**:

- Enter any addresses you want to exclude from exploits in the **Excluded Addresses** field.
- Select whether **to ignore known fragile devices** – such as printers.

8. Under the **Payload Settings**:

   - Click the **Payload Type** dropdown button to select whether the payload is **Meterpreter** or **Command shell**.
   - Click the **Connection Type** dropdown button to select whether the connection type is **reverse**, **bind**, or **auto** (determined by Metasploit Express).
   - Enter the port or range of ports that will be used for reverse connect payloads in the **Listener Ports** field. You may need to define more than one port for some exploits.
   - Enter the IP address for the payload to connect back with in the **Listener Host** field

9. Under the **Exploit Selection** section:

   - Enter any ports you want explicitly include in the exploit in the **Included Ports** field. The default setting is 1-65535.
   - Enter any ports you want to exclude from the exploit in the **Excluded Ports** field.

   - Select whether to **Skip exploits that do not match the host OS**.
   - Select whether to **Match exploits based on open ports**.
   - Select whether to **Match exploits based on vulnerability references**.

10. Under the **Advanced Settings** section:

    - Select the number of exploits you wish to run concurrently from the **Concurrent Exploits** dropdown menu. The range is 1-10 simultaneous exploits.
    - Enter the maximum amount of time (in minutes) each exploit can run in the **Timeout in Minutes** field.
    - Click the **Transport Evasion** dropdown button to select whether it is low, medium, or high.

      - **Low** – Inserts delays between TCP packets.
      - **Medium** – Transmits small TCP packets.
      - **High** – Transmits small TCP packets and inserts delays between them.

    - Select whether only **one session per target** should be obtained.
    - Select whether to perform a **dry run** of the exploit. This will provide you with details of the exploit, but will not actually run it.

11. Choose one of the following options:

    - Click the **Exploit** button. This option will run all exploits.
    - Click the **Choose Exploits** button. This option will allow you to select the exploits you want to run. Once you have selected your exploits, click the **Launch Exploits** button.

Manual Exploitation

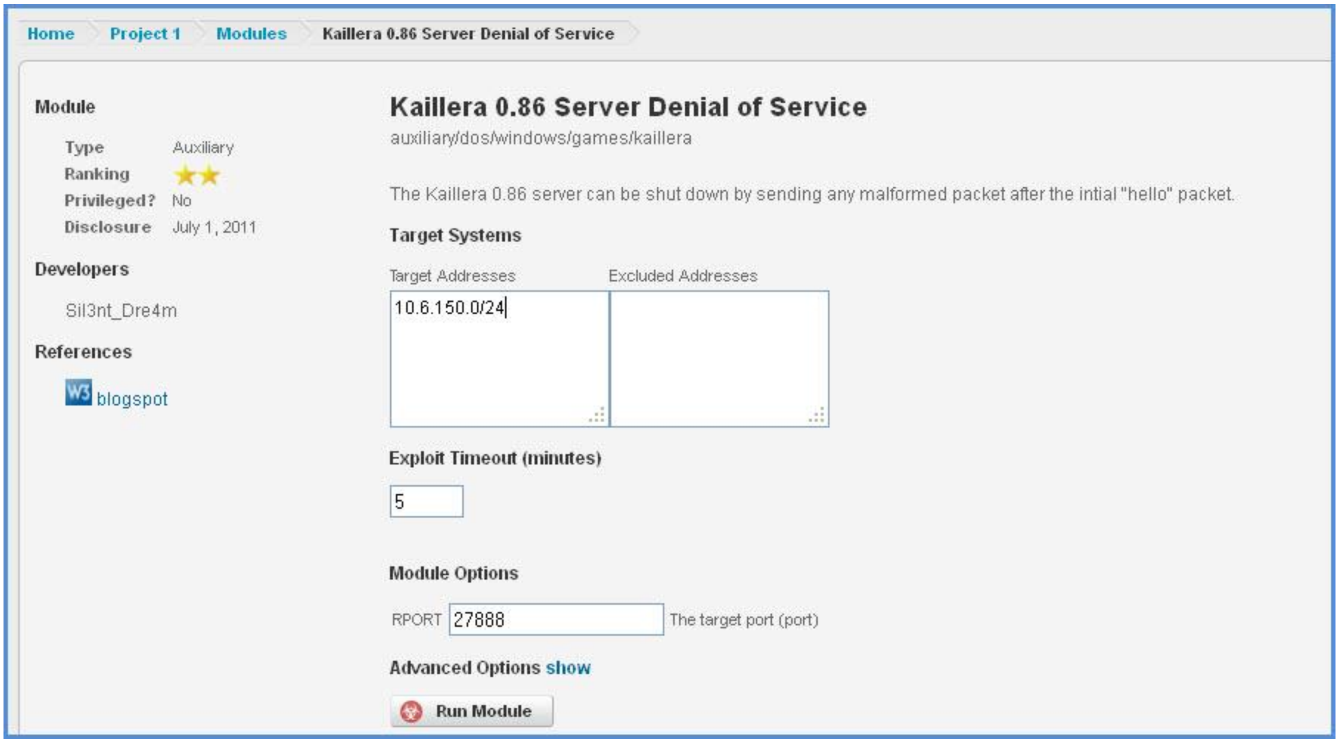
Manual exploitation provides more granular control over the modules that are used in your exploits. This method of gaining access enables you to select the modules and define the module and evasion options.

In the same way that you would select exploit modules using the automated method, you can use the same steps to determine which modules would best suit your test scenario and test requirements.

Note: Options and instructions will vary between modules – depending on the type of module (e.g., server exploit, auxiliary, client exploit); therefore, use the instructions below as a guideline for running your exploits.

You will need to:

- Create a list of system targets.
- Create a map of all available exploits using references, ports, and service names.
- Create a match table of exploits for systems – excluding devices that are fragile or cannot be exploited.
- Create a prioritized queue of exploit modules based on reliability, interleaving exploits between hosts.
- Execute exploit modules until a session I obtained.



Module

Type Auxiliary
Ranking ★★
Privileged? No
Disclosure July 1, 2011

Developers

Sil3nt_Dre4m

References

blogspot

Kaillera 0.86 Server Denial of Service

auxiliary/dos/windows/games/kaillera

The Kaillera 0.86 server can be shut down by sending any malformed packet after the intial "hello" packet.

Target Systems

Target Addresses: 10.6.150.0/24

Excluded Addresses:

Exploit Timeout (minutes): 5

Module Options

RPORT 27888 The target port (port)

Figure 17: Manual Exploitation

To manually run an exploit:

1. Select a project from the **Projects** list. This will open the project's **Overview** page.
2. Click the **Modules** tab.

3. Enter a keyword in the **Search Modules** field to search for a specific module. Use the keyword tags (i.e., name, path, platform, type, app, author, cve, bid, and osvdb) to create your search terms. Hit the **Enter** key to perform the search.
4. Select a module by clicking the module name. The module's description page will display.
5. Specify any target hosts and excluded hosts, if available.
6. Set the payload options, if available.
7. Set the **Module** Options. These vary from module to module. See the contextual help for more information about each option.
8. Set the **Advanced Options**. Advanced options vary from module to module depending on the exploit used; however descriptions for each option are provided next to the option name.
9. Set the **Evasion Options**. Evasion options vary from module to module, depending on the exploit used; however, descriptions of each evasion option are provided next to the option name.
10. Click the **Launch Attack** button.

Bruteforcing Hosts

In Metasploit Express, the Bruteforce task attempts a large number of common username and password combinations to gain access. You can use a number of preset bruteforce profiles that allow you to tailor the attack to the appropriate environment. Alternatively, credentials can be supplied through the import interface. Additionally, you can utilize your own wordlists (see 'Using your own credentials' below)

Metasploit Express will color-code bruteforce task logs to help you identify successes and failures. All successes will be recorded in the database as authentication notes, and you will be alerted via the Hosts Tab.

- **Green Messages** - Good Status Indicator
- **Red Messages** – Bad Status Indicator
- **Yellow Messages** – Credential found Indicator

Additionally, when a successful credential is identified in a session-capable (See **Supported Targets** for more information) module such as SMB, SSH, Telnet, or MSSQL a session will be automatically opened in the interface.
In the interface, you can select services you want to target in the bruteforce. Your choices are SMB, Postgres, DB2, MySQL, MSSQL, HTTP, HTTPS, SSH, Telnet, FTP, Exec, Login, Shell, VNC, and SNMP. The table shows the lockout risk of each service.

To Bruteforce hosts:

1. Select a project from the **Projects** list.
2. Click the **Hosts** tab. This will open the **Hosts** page. If you have not run a discovery scan yet, you should do so at this time.

3. Select the hosts you would like to bruteforce. Use the **Toggle** button to select or deselect all.
4. Click the **Bruteforce** button.
5. The **Target Addresses** field will be populated with the hosts found in the last scan. You can edit this list by adding and removing addresses.
6. Enter any hosts you would like to exclude from the bruteforce attack in the **Excluded Addresses** field.
7. Add your own credentials to the **Additional Credentials** field. Use the following format for your credentials: `username password`.
8. Select the **Target Services** you want to target in the bruteforce. Your choices are SMB, Postgres, DB2, MySQL, MSSQL, Oracle, HTTP, HTTPS, SSH, Telnet, FTP, EXEC, Login, Shell, VNC, and SNMP. The table shows the lockout risk of each service.
9. Select the **Depth** of the bruteforce. You can choose from:
    - **Quick –** Tries a small static list of known credentials
    - **Normal –** Tries a fixed maximum number of credentials or few protocol-specific usernames and many common passwords.
    - **Defaults Only** – Tries common default user accounts for a variety of devices, including known backdoor passwords
    - **Deep –** Tries three times as many passwords as Fast, but this will not work with slow services such as Telnet and SSH.
    - **Known Only –** Only tries credentials that were discovered in previous bruteforce tests. Note that all the other strategies are prepended with known credentials.
    - **Imported Only –** Only tries credentials that were manually imported through the Manage Credentials screen.
10. Set the **Speed** for the bruteforce requests:
    - **Turbo –** Only recommended for testing a fast LAN.
    - **Fast –** Works well for scans across most LANs.
    - **Normal –** Recommended for external use.
    - **Stealthy –** Useful across slow WAN links or to hide the scan.
    - **Slow –** Very stealthy but requires some time.
    - **Glacial –** Requires the most amount of time to complete.
11. Enter the **SMB Domains**.
12. Select the **Automatically open sessions with guessed credentials** option if you would like Metasploit Express to automatically open sessions with guessed credentials. If selected, you will find them under the **Sessions** tab after the bruteforce is complete.
13. Select the **Limit to one cracked credential per service** option if you would like Metasploit Express to have one cracked credential per service.
14. Select the **Dry Run** option if you would like to generate credentials for sessions, but do not want to authenticate them.
15. Configure the bruteforce limiters by setting the:
    - Maximum number of guesses per service

- Maximum number of password attempts per user
- Timeout in minutes per service
- Timeout in minutes overall
- Maximum number of guess overall

Note: If any of these fields is set to **0**, the limiter will not be used.

16. Configure the payload options by:
    - Choosing the **Payload type**; this can be **Meterpreter** or **Command Shell**.
    - Selecting a **Connection type**; this can be **Auto**, **Reverse**, or **Bind**. If left as **Auto**, the connection type will use **Bind** when NAT is detected and all ports on the target system are unfiltered; otherwise, it will use **Reverse**.
    - Specify the **Listener Ports**.
    - Specify the **Listener Host**.
17. Configure the **Credential Generation Switches** by enabling or disabling any of the following options:
    - Include known credentials
    - SMB: Preserve original domain names
    - Skip blank password generation
    - Exclude machine names as passwords
    - Skip common Windows machine accounts
    - Skip common Unix machine accounts
    - Recombine known, imported, and additional credentials
18. Click the **Launch Bruteforce** button.

Importing Credentials for Bruteforce

Credentials can be automatically imported for bruteforce by placing them in a specified file with the correct format in the $INSTALL_ROOT/apps/pro/msf3/data/ directory. On Windows the default $INSTALL_ROOT is C:\metasploit\ and on Linux, the default $INSTALL_ROOT is /opt/metasploit-3.7.1/):
$PROTOCOL can be one of: ssh | telnet | smb | http | https | mysql | mssql | db2 | postgres | tomcat_mgr | ftp | shell | login | exec | vnc | snmp

- **To import usernames**: Place usernames into a file within the $INSTALL_ROOT/apps/pro/msf3/data/wordlists directory with the following naming convention: $PROTOCOL_default_users.txt where $PROTOCOL is the specific protocol to which you'd like to add the usernames. The file should have only a single username on each line
- **To import passwords**: Place passwords into a file within the $INSTALL_ROOT/apps/pro/msf3/data/wordlists directory with the following naming convention: $PROTOCOL_default_pass.txt where $PROTOCOL is the specific protocol to which you'd like to add the passwords. The file should have only a single password on each line.

- **To import usernames and passwords**: Place username and password combinations into a file within the $INSTALL_ROOT/apps/pro/msf3/data/wordlists directory with the following naming convention: $PROTOCOL_default_userpass.txt where $PROTOCOL is the specific protocol to which you'd like to add the usernames and passwords. These files should be formatted with a "username password" combination on each line.

For example, if you would like to include the username password combination "rapid7 metasploit" on a smb brute, place them in the file **`C:\metasploit\apps\pro\msf3\data\wordlists\smb_default_userpass.txt`** on Windows and **`/opt/metasploit-3.7.1/apps/pro/msf3/data/wordlists/smb_default_userpass.txt`** (the application does not need to be restarted).

Utilizing a _userpass file will generate 1 username and password combination for each entry. This is a good way to test a single user. If, instead, you place the password in the _password file, it will generate 1 username and password combination for each username in the _user file. It's dependent on what you want to test, and is worthy of some consideration before adding credentials to your bruteforce.

With all current bruteforce schemes, there are some built-in caps on credential generation for each scheme, to prevent Metasploit from generating too many combinations to be useful.

Importing Credentials Using the Advanced Credentials Management Interface

If you are importing large sets of untested credentials or you are running scans in **normal**, **deep**, and **import only** modes, use the **Advanced Credential Management** interface.

If you import multiple files, Metasploit Express will consolidate the credentials from each file and store the data as one running file. The imported credentials will not display under the credentials area; however, they can be downloaded and viewed as a single text file.

Note: The **Additional Credentials** field should only be used for known credentials and for bruteforce attacks running with the **Include known credentials** option enabled.

To add a set of imported credentials:

1. Select a project from the **Projects** list.
2. Click the **Hosts** tab. This will open the **Hosts** page. If you have not run a discovery scan yet, you should do so at this time.
3. Select the hosts you would like to bruteforce. Use the **Toggle** button to select or deselect all.
4. Click the **Bruteforce** button.
5. Scroll down to the bottom of the **Bruteforce Attack** page and locate the **Advanced Credentials Management** area.
6. Click the **Manage Credentials** button. The Credential Import page will display.
7. Click the **Browse** button to navigate to the location of the credentials file. The credentials file must be in plain ASCII.

8. Click the **Open** button once the credentials file has been selected.
9. Click the **Upload** button to import the credentials file.

Viewing Imported Credentials

All imported credential data can be downloaded and viewed as a single text file.

To view imported credentials:

1. Select a project from the **Projects** list. This will open the project's **Overview** page.
2. Click the **Bruteforce** button located on the **Project Overview** page.
3. Scroll down to the bottom of the **Bruteforce Attack** page and locate the **Advanced Credentials Management** area.
4. Click the **Manage Credentials** button. The **Credential Import** page will display.
5. Click the **Download** button.
6. Save the file to a location on your computer.

Deleting Imported Credentials

Deleting credentials will remove all imported credential data from your system.

To delete imported credentials:

1. Select a project from the **Projects** list. This will open the project's **Overview** page.
2. Click the **Bruteforce** button located on the **Project Overview** page.
3. Scroll down to the bottom of the **Bruteforce Attack** page and locate the **Advanced Credentials Management** area.
4. Click the **Manage Credentials** button. The **Credential Import** page will display.
5. Click the **Delete All** button.

Credential Generation Switches

Using any of the Credential Generation Switches, you can specify how credentials are generated by Metasploit Pro. This option is available for bruteforcing tasks.

The following options are available:

- **Include known credentials** – Uses all credentials already in the project. These credentials are tried first. All credentials with the "known only" and "quick" are not affected by the Credential Generation Switch.

- **SMB: Preserve original domain names** – Tries the original domain name. 7

- **Skip blank password generation** – Disables using blank passwords.

- **Exclude machine names as passwords** – Skips using known computer names and user names as passwords.

- **Skip common Windows machine accounts** – Skips Windows accounts that don't have remote login rights or randomly generated passwords. These include: TsInternetUser krbtgt NetShowServices, IUSR_<anything>, IWAM_<anything>, WMUS_USER-<anything>.

- **Skip common Unix machine accounts** – Skips Unix accounts that don't have remote login rights or randomly generated passwords. This includes: daemon, bin, sys, sync, games, man, lp, mail, news, uucp, proxy, www-data backup list, irc, gnats, nobody, libuuid, syslog, messagebus, haldaemon, hplip, avahi, couchdb, kernoops, saned, pulse, gdm, sshd, telnetd, dhcp, avahi-autoipd, speech-dispatcher.

- **Recombine known, imported, and additional credentials** – Takes all the usernames:passwords from the known credentials list, imported list, and credentials textbox, and assigns all the passwords to all users.

Manual Exploitation

Manual exploitation provides more granular control over the modules that are used in your exploits. This method of gaining access enables you to select the modules and define the module and evasion options.

In the same way that you would select exploit modules using the automated method, you can use the same steps to determine which modules would best suit your test scenario and test requirements.

You will need to:

- Create a list of system targets.
- Create a map of all available exploits using references, ports, and service names.
- Create a match table of exploits for systems – excluding devices that are fragile or cannot be exploited.
- Create a prioritized queue of exploit modules based on reliability, interleaving exploits between hosts.
- Execute exploit modules until a session I obtained.

To run a manual exploit:

1. Select a project from the **Projects** list. This will open the project's **Overview** page.
2. Click the **Modules** tab.

3. Enter a keyword in the **Search Modules** field to search for a specific module. Use the keyword tags (i.e., name, path, platform, type, app, author, cve, bid, and osvdb) to create your search terms. Hit the **Enter** key to perform the search.
4. Select a module by clicking the module name. The module's description page will display.
5. Enter the target systems (range of host addresses) in the **Target Systems** field.
6. Enter any address you want to exclude from the exploit in the **Excluded Addresses** field.
7. Enter the **Single Exploit Timeout** (in minutes).
8. Select a connection type from the **Payload Connection Method** dropdown menu.
9. Select an exploit target from the **Exploit Target** dropdown menu.
10. Set the **Module** Options:

    - **SRVHOST** – This refers to the address on which the local host will listen.
    - **SRVPORT** – This refers to the port on which the local port will listen.
    - **SSL** – Select this option to enable SSL negotiations for incoming SSL connections.
    - **SSL Version** – This refers to the version of SSL that will be used. SSL1, SSL2, and SSL3 are supported.
    - **URIPATH** – This refers to the URI that will be used for the exploit. By default, this value is random.

11. Set the **Advanced Options**. Advanced options vary from module to module depending on the exploit used; however descriptions for each option are provided next to the option name.
12. Set the **Evasion Options**. Evasion options vary from module to module, depending on the exploit used; however, descriptions of each evasion option are provided next to the option name.
13. Click the **Launch Attack** button.

Running Post-Exploitation Modules

Once you have gained access to a target, you have two options for post-exploitation: running scripts via command shell or running post-exploitation modules. Post-exploitation modules provide a standardized interface to perform post-exploit attacks, which makes it a simpler alternative to the command line.

Each open session will display a list of post-exploitation modules that are applicable for that session (e.g., based on session type, services, etc.).

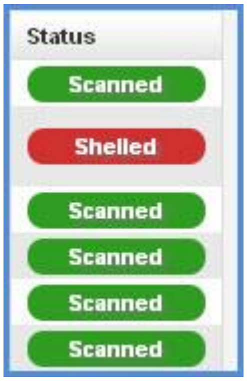
To run post-exploitation modules:

1. Click on the **Sessions** tab.
2. Click on a session name from the **Active Sessions** list.

3. Click on the **Post-Exploitation Modules** tab, located at the bottom of the page next to the **Session History** tab.
4. Click on a module listed in under the **Module Title** column. The module information page will open.
5. Click the **Run Module** button.

Interpreting Host Badges

The status of each host will be listed on the **Hosts** page.



Status
Scanned
Shelled
Scanned
Scanned
Scanned
Scanned

Figure 18: Host Badges

The statuses are defined as follows:

1. **Scanned** – A device has been discovered.
2. **Cracked** – Credentials were successfully bruteforced but no session was obtained.
3. **Shelled** – An open session was obtained on the device.
4. **Looted** – Evidence has been collected from the device.

Taking Control of Sessions

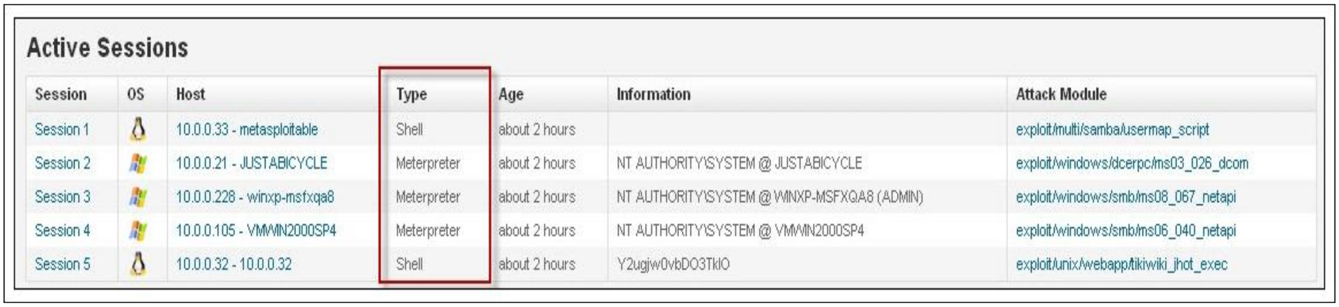
After you have discovered valid hosts on the target system and gained access to sessions on that system, you can take control of the open sessions.

There are two types of sessions:

- **Command shell sessions** – These sessions allow you to run collection scripts and give you a shell to run arbitrary commands against the host.
- **Meterpreter sessions** – These sessions are much more powerful. They enable you to gain access to the device using VNC and enable you to upload/download sensitive information using a built-in file browser.

The type of session is determined by the mechanism used to create the session and the type of environment on which the session runs; Meterpreter shells are currently only available for

Windows. To determine a session’s type, go to the **Sessions** page. You will notice that all sessions will be listed as **Meterpreter** or **Shell** under the **Type** column. If you click on the session name, you will be able to see a list of actions that can be taken against the session.



Active Sessions

Session	OS	Host	Type	Age	Information	Attack Module
Session 1	🐧	10.0.0.33 - metasploitable	Shell	about 2 hours		exploit/multi/samba/usermap_script
Session 2	⊞	10.0.0.21 - JUSTABICYCLE	Meterpreter	about 2 hours	NT AUTHORITY\SYSTEM @ JUSTABICYCLE	exploit/windows/dcerpc/ms03_026_dcom
Session 3	⊞	10.0.0.228 - winxp-msfxqa8	Meterpreter	about 2 hours	NT AUTHORITY\SYSTEM @ WINXP-MSFXQA8 (ADMIN)	exploit/windows/smb/ms08_067_netapi
Session 4	⊞	10.0.0.105 - VMWIN2000SP4	Meterpreter	about 2 hours	NT AUTHORITY\SYSTEM @ VMWIN2000SP4	exploit/windows/smb/ms06_040_netapi
Session 5	🐧	10.0.0.32 - 10.0.0.32	Shell	about 2 hours	Y2ugjw0vbDO3TkIO	exploit/unix/webapp/tikiwiki_jhot_exec

Figure 19: Session Type

Command Shell Vs. Meterpreter Sessions

A command shell session will be created under the following conditions:

- Successful exploit on *nix
- SSH bruteforce on *nix
- Telnet bruteforce on *nix
- Tomcat bruteforce on *nix

A Meterpreter session will be created under the following conditions:

- Successful exploit on Windows
- SSH bruteforce on Windows
- Telnet bruteforce on Windows
- SMB bruteforce on Windows
- Tomcat bruteforce on Windows

All other successful authentication will result in an authentication note attached to the host, and an entry in the corresponding reports. Some protocols and servers do not allow you to execute commands directly. For example, you can utilize FTP to bruteforce credentials, but once a valid credential is found, commands cannot be run directly on the server, thus, no session can be obtained.

When cases like this are identified during a bruteforce or an exploit, an alert appears next to your project’s **Hosts** tab indicating that a valid account was identified, but that a session was not able to be created. If new credential information is found for a particular host, you can utilize these credentials to authenticate to the host outside of Pro.

Interacting with Command Shell Sessions

To manipulate a Command Shell session:

1. Click the **Sessions** tab.
2. Click on the active session you would like to work with. The session must be a **Shell** type. A **Session** details page will open.
3. Under the **Available Actions** section of the Sessions detail page, click the **Command Shell** button.

A simulated command shell will open in a new tab on your browser. This command shell functions as terminal emulator and can be used to run any non-interactive process on the target host.

Interacting with Meterpreter Sessions

To manipulate a Meterpreter session:

1. Click the **Sessions** tab.
2. Click on the active session you would like to work with. The session must be a **Meterpreter** type. A **Session** details page will open.
3. Under the **Available Actions** section of the **Session** detail page, click the **Virtual Desktop** button.
4. Choose either the Java client or choose to manually connect to an external client.

Note: In order to interact with a Meterpreter session, you must have a session on an exploited Windows target open.

Viewing Session Details

Active sessions are sessions that were successfully opened during the bruteforce or exploitation of a host or when a background module – such as a browser exploit – succeeds in exploiting a client system. You can view all active and closed sessions on the **Sessions** page.

To view a session's details:

1. Click on a session name to see more information on a specific session – such as the session type and attack module used. Additionally, you can perform additional actions on the session – such as collecting the system data, accessing the virtual desktop, accessing and searching the file system, running a command shell, creating a pivot point, and closing the session.

Obtaining VNC Sessions

With Meterpreter sessions, you can obtain a VNC session to any host with an open session. You are provided with two methods of connecting to the remote desktop: to manually connect to the desktop using the provided address configuration or you can connect using a Java Applet.

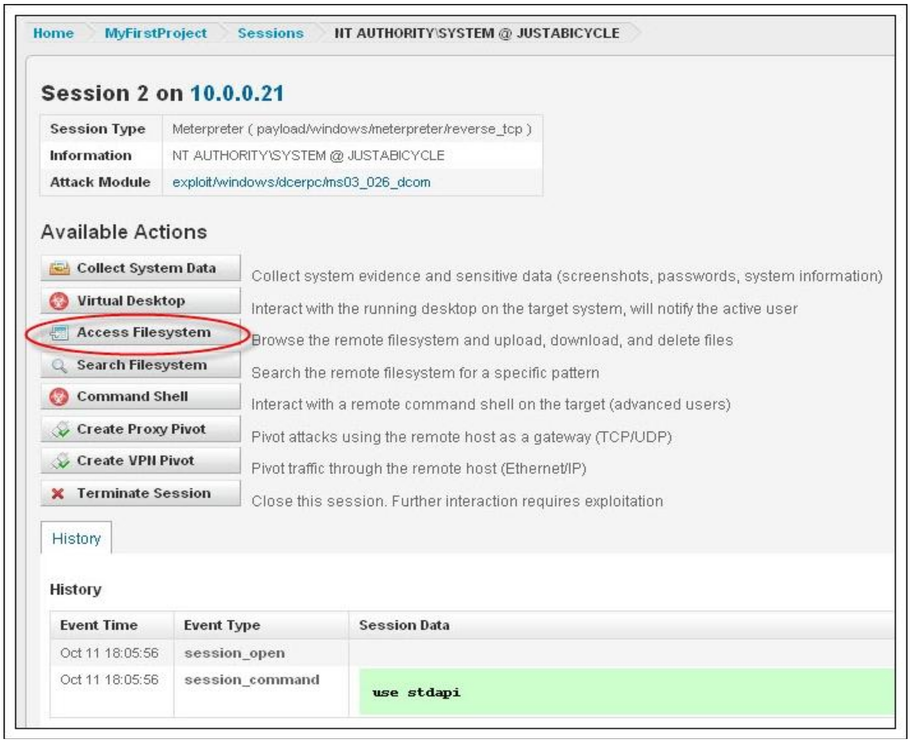
Metasploit Express contains a VNC client in the form of a Java applet. Please install the latest Java for your platform at: http://www.java.com/en/download/manual.jsp. Additionally, an external client – such as VNC Viewer – can be used.

To obtain a VNC session:

1. Click the **Sessions** tab.
2. Click on an active session. A **Session** details page will open.
3. Click the **Virtual Desktop** button to connect to the remote desktop.
4. Click **OK** with the **Virtual Desktop** confirmation window appears.
5. Choose whether to **Connect manually** to the remote desktop or to use a **Java Applet**.

Accessing a Filesystem

For Meterpreter sessions, you can use the Metasploit Express interface directly to browse the file system. You can also upload, download, or delete any files to the filesystem.



Session 2 on 10.0.0.21

Session Type	Meterpreter (payload/windows/meterpreter/reverse_tcp)
Information	NT AUTHORITY\SYSTEM @ JUSTABICYCLE
Attack Module	exploit/windows/dcerpc/ms03_026_dcom

Available Actions

Collect System Data	Collect system evidence and sensitive data (screenshots, passwords, system information)
Virtual Desktop	Interact with the running desktop on the target system, will notify the active user
Access Filesystem	Browse the remote filesystem and upload, download, and delete files
Search Filesystem	Search the remote filesystem for a specific pattern
Command Shell	Interact with a remote command shell on the target (advanced users)
Create Proxy Pivot	Pivot attacks using the remote host as a gateway (TCP/UDP)
Create VPN Pivot	Pivot traffic through the remote host (Ethernet/IP)
Terminate Session	Close this session. Further interaction requires exploitation

History

Event Time	Event Type	Session Data
Oct 11 18:05:56	session_open	
Oct 11 18:05:56	session_command	use stdapi

Figure 20: Access the file system

To access the filesystem:

1. Click the **Sessions** tab.
2. Click on an active session. A **Session** details page will open.
3. Click the **Access Filesystem** button located under the **Available Actions** area. A new window will open, displaying the remote filesystem.

Uploading Files to a Remote Filesystem

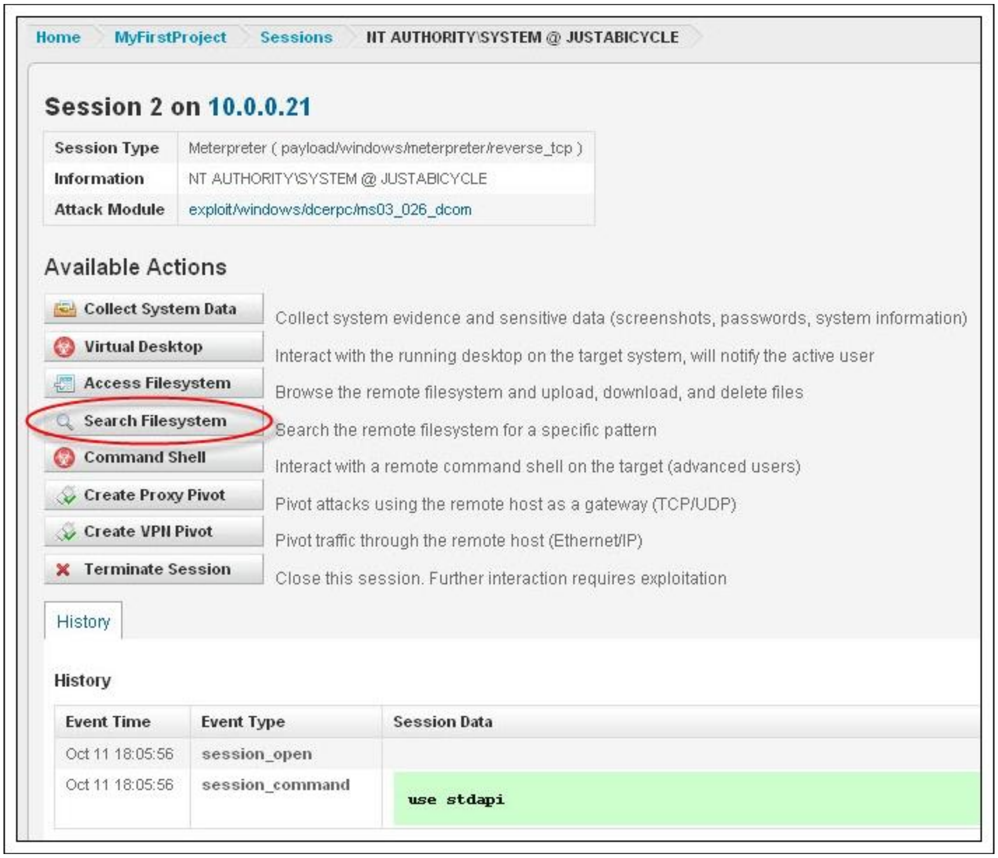
For Meterpreter sessions, you can use the Metasploit Express interface to upload files to a remote filesystem.

To upload files to a remote filesystem:

1. Click the **Sessions** tab.
2. Click on an active session. A **Session** details page will open.
3. Click the **Access Filesystem** button located under the **Available Actions** area. A new window will open, displaying the remote filesystem.
4. Select the directory to which you would like to upload the file. You can do this by manually entering in a directory path or by navigating through the directory and selecting directory paths.
5. Click the **Upload** link.
6. Click the **Browse** button to navigate to the location of the file to be uploaded. Once you have located the file, select it, and click the **Open** button.
7. Enter a name for the file in the **File Name** field. If you do not specify one, then it will be named **empty** by default.
8. Select whether to **run the file** after it is uploaded to the filesystem.
9. Click the **Upload** button.

Searching a Filesystem

For Meterpreter sessions, you can use the **Search Filesystem** action to locate files by name.



Session 2 on 10.0.0.21

Session Type	Meterpreter (payload/windows/meterpreter/reverse_tcp)
Information	NT AUTHORITY\SYSTEM @ JUSTABICYCLE
Attack Module	exploit/windows/dcerpc/ms03_026_dcom

Available Actions

Collect System Data	Collect system evidence and sensitive data (screenshots, passwords, system information)
Virtual Desktop	Interact with the running desktop on the target system, will notify the active user
Access Filesystem	Browse the remote filesystem and upload, download, and delete files
Search Filesystem	Search the remote filesystem for a specific pattern
Command Shell	Interact with a remote command shell on the target (advanced users)
Create Proxy Pivot	Pivot attacks using the remote host as a gateway (TCP/UDP)
Create VPN Pivot	Pivot traffic through the remote host (Ethernet/IP)
Terminate Session	Close this session. Further interaction requires exploitation

History

Event Time	Event Type	Session Data
Oct 11 18:05:56	session_open	
Oct 11 18:05:56	session_command	use stdapi

Figure 21: Search the file system

To search the File System:

1. Click the **Sessions** tab.
2. Click on an active session. A **Session** details page will open.
3. Click the **Search Filesystem** button. A new window will open, displaying the remote filesystem.
4. Enter the name of the file you would like to find in the **Search Files** field.
5. Hit the **Enter** key.

Replaying Tasks

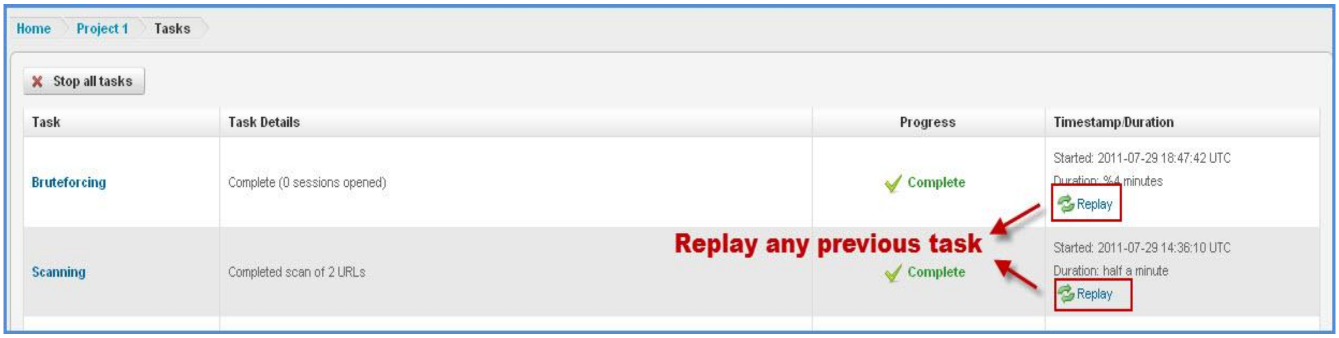
The Replay feature enables you to essentially “replay” a specific task that has already been performed. These tasks include:

- Scanning (discovering)
- Bruteforcing
- Exploiting
- Collecting
- Cleaning up

- WebScanning
- WebAuditing
- WebSploiting

You can access the Replay feature from the **Tasks** tab of your project page. A list of previously run tasks will be displayed in the **Tasks** window. The Replay feature is located under the **Timestamp/Duration** column for each task. Clicking **Replay** will open the original configuration page for that specific task.

Note: For some tasks (e.g., exploiting, discovering), you will need to click on the **Advanced Options** button to see the available configuration options.



Task	Task Details	Progress	Timestamp/Duration
Bruteforcing	Complete (0 sessions opened)	✓ Complete	Started: 2011-07-29 18:47:42 UTC Duration: %4 minutes Replay
Scanning	Completed scan of 2 URLs	✓ Complete	Started: 2011-07-29 14:36:10 UTC Duration: half a minute Replay

Replay any previous task

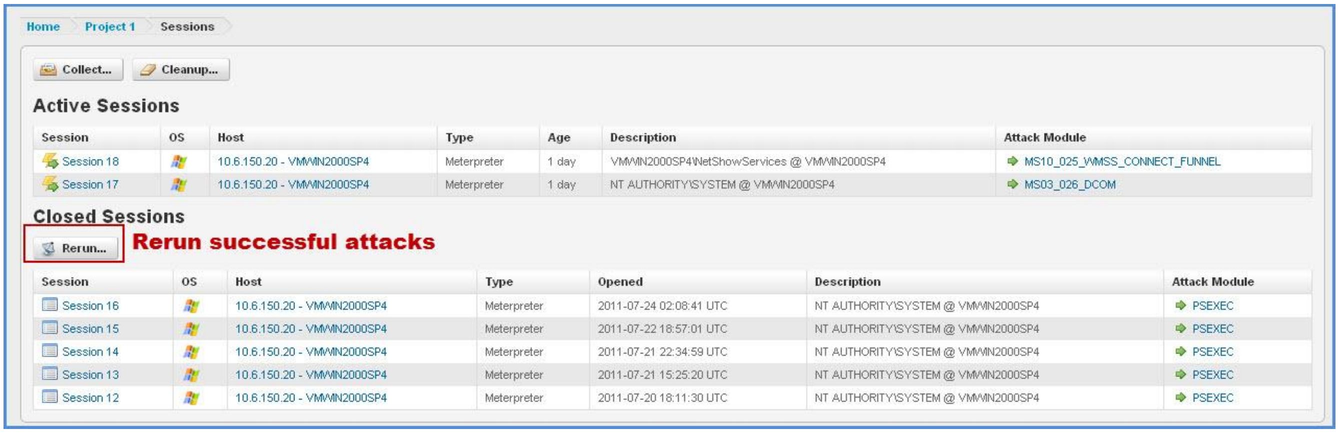
Figure 22: Replay tasks

To replay a task:

1. Click on the **Tasks** tab from your project page.
2. Locate the task you want to replay (e.g., bruteforcing, exploiting, discovering, etc.).
3. Click **Replay** for that task. A configuration page for that task will display. For example, if you choose a bruteforcing task, the original configuration page for the bruteforce attack will display. From here, you can modify any settings for the task or leave them in their original settings.
4. Click the task related button (e.g., Exploit, Launch Bruteforce, Launch Scan) when you are ready to replay the task.

Rerunning Attacks

The Rerun feature enables you to instantly rerun all previous exploit modules that successfully opened sessions.



Active Sessions

Session	OS	Host	Type	Age	Description	Attack Module
Session 18		10.6.150.20 - VMWIN2000SP4	Meterpreter	1 day	VMWIN2000SP4\NetShowServices @ VMWIN2000SP4	MS10_025_WMSS_CONNECT_FUNNEL
Session 17		10.6.150.20 - VMWIN2000SP4	Meterpreter	1 day	NT AUTHORITY\SYSTEM @ VMWIN2000SP4	MS03_026_DCOM

Closed Sessions

Rerun successful attacks

Session	OS	Host	Type	Opened	Description	Attack Module
Session 16		10.6.150.20 - VMWIN2000SP4	Meterpreter	2011-07-24 02:08:41 UTC	NT AUTHORITY\SYSTEM @ VMWIN2000SP4	PSEXEC
Session 15		10.6.150.20 - VMWIN2000SP4	Meterpreter	2011-07-22 18:57:01 UTC	NT AUTHORITY\SYSTEM @ VMWIN2000SP4	PSEXEC
Session 14		10.6.150.20 - VMWIN2000SP4	Meterpreter	2011-07-21 22:34:59 UTC	NT AUTHORITY\SYSTEM @ VMWIN2000SP4	PSEXEC
Session 13		10.6.150.20 - VMWIN2000SP4	Meterpreter	2011-07-21 15:25:20 UTC	NT AUTHORITY\SYSTEM @ VMWIN2000SP4	PSEXEC
Session 12		10.6.150.20 - VMWIN2000SP4	Meterpreter	2011-07-20 18:11:30 UTC	NT AUTHORITY\SYSTEM @ VMWIN2000SP4	PSEXEC

Figure 23: Rerun attacks

To rerun the previous attack:

1. Click on the **Sessions** tab from your project page.
2. Click the **Rerun** button located under the **Closed Sessions** area. A new page will display the **Automated Attack Rerun Settings**.
3. Click the **Payload Type** dropdown button to choose a payload type being used. You can choose from **Meterpreter** or **Command Shell**.
4. Click the **Connection Type** dropdown button to choose a connection type. You can choose from Auto, Reverse, or Bind.
5. Enter the port or range of ports that will be used for reverse payloads in the **Listener Ports** field.
6. Enter the IP address for the payload to connect back with in the **Listener Host** field. This field is only necessary when the address needs to be overridden.
7. Click the **Rerun Attacks** button.

Collecting Evidence and Session Cleanup

Metasploit Express can automatically collect system data from exploits on target systems after gaining access. Metasploit refers to collected system data as evidence.

Evidence is an indicator of the success of exploits and can be used for further analysis and penetration. The evidence typically includes system information, screenshots, password hashes, SSH keys, and other sensitive information.

Collecting Evidence for a Project

To collect system data for a project:

1. Click on the **Sessions** tab.
2. Click the **Collect** button located under the **Evidence Collection** pane.

3. Select the sessions from which you want to collect exploit evidence. Use the Toggle option to select or deselect all sessions.
4. Choose whether or not to **collect system information**.
5. Choose whether or not to **collect system passwords**.
6. Choose whether or not to include **screenshots**.
7. Choose whether or not to collect **SSH keys**.
8. Choose whether or not to collect **other files** besides the above.
9. Enter a regex or a set of characters to filter the results by a filename pattern in the **Filename Pattern** field.
10. Enter the maximum file count to collect per session in the **Maximum File Count** field.
11. Enter the maximum file size to include per session, in kilobytes, in the **Maximum File Size** field.
12. Click the **Collect Data** button.

Evidence collection will begin and you can review the progress by clicking the **Task** tab.

Collecting Evidence for Active Sessions

To collect evidence for individual active sessions:

1. Click the Sessions tab.
2. Click on an active session.
3. Click the Collect System Data button located under Available Actions.
4. Select the Active Sessions for which to run the data collection.
5. Choose whether or not to collect system information.
6. Choose whether or not to collect system passwords.
7. Choose whether or not to include screenshots.
8. Choose whether or not to collect SSH keys.
9. Choose whether or not to collect other files besides the above.
10. Enter a regex or a set of characters to filter the results by a filename pattern in the Filename Pattern field.
11. Enter the maximum file count to collect per session in the Maximum File Count field.
12. Enter the maximum file size to include per session, in kilobytes, in the Maximum File Size field.
13. Click the Collect Data button.

Viewing Collected Evidence

Reports are auto-generated any time a task takes place that updates the database. Evidence can be reviewed from the **Reports** area of the project. Selecting the **Collected Evidence** live report will instantly show you the collected evidence from the compromised hosts.

Cleaning Up (or Closing) Active Sessions

Sessions that have been bruteforced and exploited will need to be closed and cleaned up. During cleanup, sessions that were open will be closed.

To clean up evidence for a project:

1. Click on the **Overview** tab.
2. Click the **Cleanup** button located under the **Cleanup** area. The Compromised Host Cleanup window will display.
3. Select the sessions you would like to cleanup.

Reporting

You have two options for viewing reports: you can either view a live report, which details the most current test information and statistics, or you can generate a report, which you can download and export to multiple formats (e.g., PDF, Word, RTF, XML, etc.). These reports summarize all the information discovered during the penetration test.

Viewing Live Reports

Live reports include:

- **Executive Summary**: A high-level summary of the actions taken during the project and the results.
- **Detailed Audit Report**: A large report containing every detail of the this project
- **Compromised Hosts**: A report focused on the systems compromised
- **Network Services**: A report focused on the exposed network services
- **System Evidence**: A report focused on the data collected from compromised systems
- **Authentication Tokens**: A report focused on the usernames and passwords obtained

To view a live report:

1. Click the **Reports** tab.
2. Click on any of the live report names (e.g., Executive Summary, Detailed Audit Report, Collected Evidence, etc.).

Creating Custom Live Reports

The live reports can be further customized if desired. For most reports, you can mask the user names and passwords and filter the addresses included in the report. For the **Collected Evidence** report, you can also elect to exclude screenshots and passwords.

To create a custom live report:

1. Click the **Reports** tab.
2. Click any of the reports located under the **Customize** field (e.g., Customized Executive Summary, Customized Detailed Audit Report, etc.). A Customized Report window will open, enabling you to mask usernames/passwords and filter addresses included in the live report.

Generating Reports

The reports page also provides the opportunity to create and store generated reports, which are PDF, XML, and ODT reports that summarize all the findings in the penetration test.

- **PDF Report** - Generate a full project report in pdf-format.
- **Word Report –** Allows you to generate a report in an editable format.
- **XML Report** – Allows you to generate results in a machine-consumable format.
- **ZIP Report** – Allows you to share results with clients or other testers.
- **Replay (scripts)** – Generate an .rc script suitable for replay with msfconsole.

To manually generate a report for a project:

1. Click the **Reports** tab.
2. Click on the **Generate a Report** button located under the **Generated Reports** are of the **Reports** page. The **Report Generator** window will open.
3. Select the desired report format from the **Report Format** dropdown menu.
4. Enter in the IP addresses you wish to include or exclude under the **Included Addresses** and **Excluded Addresses** fields.
5. Select the **Mask usernames/passwords** option if you wish to hide usernames and passwords.
6. Click the **Generate** button**.**

Reports will be archived on the Metasploit Express server and can be downloaded at any time.

Downloading Reports

To download a report:

1. Click the **Reports** tab.
2. Locate the report you want to download from the **Generated Reports** area.
3. Click the corresponding **Download** button. A new window will open, prompting you to choose to open or save your report.
4. Click **OK**.

Exporting Replay Scripts

To export replay scripts:

1. Click the **Reports** tab.
2. Click on the **Generate a Report** button located under the **Generated Reports** are of the **Reports** page. The **Report Generator** window will open.
3. Choose **Replay (Scripts)** from **the Select a Report Format** dropdown menu.
4. Enter in the IP addresses you wish to include or exclude under the **Included Addresses** and **Excluded Addresses** fields.
5. Select the **Mask usernames/passwords** option if you wish to hide usernames and passwords.
6. Click the **Generate** button.

After the report has finished generating, you will need to download the report from the **Generated Reports** area.

Deleting Reports

To delete a report:

1. Click the **Reports** tab.
2. Locate the report you want to delete from the **Generated Reports** area.
3. Click the corresponding **Delete** button. A new window will open, prompting you to confirm the deletion.
4. Click **OK**.

Working with Modules

Metasploit Express performs the tasks (discover, bruteforce, etc.) functionality in the form of modules. These modules automate the functionality provided in the open source framework, and make it simpler to perform multiple related tasks.

Searching for Modules

To search for modules:

1. Click on the **Modules** tab.
2. Enter a keyword expression in the **Search Modules** field to search for a specific module. Use the **Search Keywords** table located directly below the search field to create the desired keyword expression (e.g., name:Microsoft, cve:2008).
3. Hit **Enter** to perform the search.

When the results are returned, you can click on any **Module** name to view more detailed information about that module and view all the configurable options for a manual attack.

Manually Launching an Exploit

Manual exploitation of a host allows you to select the specific module that will be used to exploit the host. To do this, you will need to first search for the module you want to use; then, you can launch the attack directly from the individual module's details page.

To manually launch an exploit:

1. Click on the **Modules** tab.
2. Enter a keyword expression in the **Search Modules** field to search for a specific module. Use the **Search Keywords** table located directly below the search field to create the desired keyword expression (e.g., name:Microsoft, cve:2008).
3. Hit **Enter** to perform the search.
4. Click on the module you would like to use for the attack. The module's details page will open.
5. Enter the **target address range** you would like to target.
6. Enter any addresses you would like to **exclude** from the attack.
7. Enter the **single exploit timeout** (in minutes).
8. Select a **payload connection method**.
9. Select an **exploit target**.
10. Set the **Module** Options. These options will vary between modules depending on the type of exploit used.
11. Set the **Advanced Options**. Advanced options vary from module to module depending on the exploit used; however descriptions for each option are provided next to the option name.
12. Set the **Evasion Options**. Evasion options vary from module to module, depending on the exploit used; however, descriptions of each evasion option are provided next to the option name.
13. Click the **Launch Attack** button.

Viewing Module Statistics

To view module statistics:

1. Click on the Modules tab.
2. Locate the area called Module Statistics. All stats pertaining to modules will be listed here. This includes: the total number of modules, exploit modules, auxiliary modules, server-side exploits, and client-side exploits.

Task Settings

With each type of major task in Metasploit Express – such as discovery scanning, bruteforcing, host exploitation – there are a set of configurable settings that can be defined for each task. All available settings will vary from task to task. This section will provide all the configurable settings in Metasploit Express, broken down into tasks.

Discovery Scan Settings

The following table provides information on the discovery scan settings that are available.

Table 2: Discovery Scan Settings

Setting Name	Description
Target Addresses	Target addresses are the addresses that will be scanned. By default, these are pulled from **Project Settings -> Network Boundaries** and were established when the project was created.
Excluded Addresses	**Excluded Addresses** will be specifically excluded from the scan. Addresses not included in the Target Addresses field do not necessarily need to be excluded.
Additional TCP Ports	Additional TCP ports are appended to the already existing Nmap scan ports. These ports are appended to the '-p' parameter.
Excluded TCP Ports	These TCP ports are excluded from all service discovery (including all Nmap options).
Custom TCP Port Range	These TCP ports are utilized in place of the defaults. For example, specifying ports 1-20 would result in the following Nmap command: /nmap -sS - -PS1-20 -PA1-20 -PU51094 -PP -PE -PM -PI -p1-20 --host-timeout=5m -O --max-rtt-timeout=300 --initial-rtt-timeout=100 --max-retries=2 --stats-every 10s --min-rate=200 Note: If UDP Service Discovery or Identify Unknown Services is checked, then these will still run (despite Custom TCP Port Range).
Fast Detect: Common TCP Ports Only	The **Fast Detect** option enables to run a scan on the most common TCP ports, which reduces the total number of ports scanned.

Setting Name	Description
Portscan Speed (Discovery Settings)	The **Portscan Speed** setting enables you to control the Nmap timing option (-T). There are six different levels of timing templates from which you can choose: • Insane (5) – Aggressively speeds up the scan by assuming that you are on super fast network and will sacrifice accuracy for speed. This setting will not allow the scan delay to exceed 5 ms. • Aggressive (4) – Speeds up the scan by assuming that you are on a fast and reliable network. This setting will not allow the scan delay to exceed 10 ms. • Normal (3) – This is the default mode and does not affect the scan. • Polite (2) – Utilizes less bandwidth and target resources to slow down the scan. • Sneaky (1) – Used for IDS evasion. • Paranoid (0) – Used for IDS evasion.
Portscan Timeout (Discovery Settings)	The **Portscan Timeout** setting determines the amount of time Nmap spends on each hosts. By default, this value is set to five minutes.
UDP Service Discovery (Discovery Settings)	The **UDP Service Discovery** option sets the scan to find all services currently on the network.
Identify Unknown Services (Discovery Settings)	The **Identify Unknown Services** option sets the scan to find all unknown services and applications on the network.
Single Scan (Discovery Settings)	The **Single Scan** setting enables you to run a scan on each host individually. The discovery process will scan the first host entirely and store that information in the database before moving on to the next host.
Dry Run (Discovery Settings)	The **Dry Run** setting enables you to prepare the nmap command line without actually executing it.
SMB Username (Optional Settings)	The **SMB Username** field is the username that will be passed onto the Metasploit SMB enumeration modules.
SMB Password (Optional Settings)	The **SMB Password** field is the password that will be passed onto the Metasploit SMB enumeration modules.
SMB Domain (Optional Settings)	The **SMB Domain** field is the domain that will be passed onto the Metasploit SMB enumeration modules.

NeXpose Scan Settings

The following table describes the different scan settings that are available for the NeXpose scan.

Table 3: NeXpose Scan Settings

Setting Name	Description
NeXpose Scan Targets	The **NeXpose Scan Targets** field lists the target systems that you wish to scan. By default, the application uses the network boundaries.
NeXpose Server and Port	The **NeXpose Server and Port** field enables you to list the local or remote NeXpose server that will be used to perform discovery and vulnerability scanning.
NeXpose Username	This is the username that will be used to log into the NeXpose system.
NeXpose Password	This is the password that will be used to log into the NeXpose system.
Scan Credentials	Scan credentials are used to scan hosts. Multiple credentials are currently not supported; therefore, if you need to use multiple credentials, please use NeXpose directly. • **Type** – Select Windows/CIFS, Secure Shell/SSH, Telnet, HTTP, FTP, SNMP, or POP3. • **User** – The username used for the scan credentials. • **Password** – The password used for the scan credentials.
Scan Limitations	Metasploit Express currently only supports scanning the number of hosts that are licensed in NeXpose; if you supply more than your licensed number of hosts (32 in Community), the scan will fail.
Scan Template	The **Scan Template** option enables you to select the template that will be used to scan the network. Currently, only default predefined templates are supported. The following list describes each of the available **Scan Templates**: • **Penetration Test Audit** – Performs an in-depth penetration test of all systems using only safe checks. Host-discovery and network penetration options will be enabled, allowing NeXpose to dynamically discover additional systems in your network to target. In-depth patch/hotfix checking, policy compliance checking, and application-layer auditing will not be performed. • **Full Audit** – Performs a full network audit of all systems using only safe checks, including network-based

Setting Name	Description
	vulnerabilities, patch/hotfix checking, and application-layer auditing. Only default ports are scanned, and policy checking is disabled, making this faster than the Exhaustive scan. • **Exhaustive** – Performs an exhaustive network audit of all systems and services using only safe checks, including patch/hotfix checking, policy compliance checking, and application-layer auditing. Performing an exhaustive audit could take several hours or even days to complete, depending on the number of hosts selected. • **Discovery** – Performs a discovery scan to identify live devices on the network, including host name and operating system. No further enumeration, policy or vulnerability scanning will be performed. • **Aggressive Discovery** – Performs a fast and cursory discovery scan to identify live devices on high speed networks, including host name and operating system. Packets are sent at a very high rate which may trigger IPS/IDS sensors, SYN flood protection and exhaust states on stateful firewalls. No further enumeration, policy or vulnerability scanning will be performed. • **DoS Audit** – Performs a basic network audit of all systems using both safe and unsafe (denial-of-service) checks. In-depth patch/hotfix checking, policy compliance checking, and application-layer auditing will not be performed.

Bruteforce Settings

The following table describes the different scan settings that are available for bruteforcing.

Table 4: Bruteforce Settings

Setting Name	Description
Bruteforce Depth	***Quick*** Designed to identify the most basic password combinations, Quick is the shortest of the bruteforce, tries a small (<25) number of known username/password combinations. It's a static list of these credentials, tried against all discovered services:

Setting Name	Description
	• Admin:admin • Admin:admin1 • Admin:admin! • Test:test • Test:test1234 • test123:test123 • cisco:cisco • user:user • administrator:administrator • root:root • root:toor All usernames are then tried with [blank] passwords Known credentials will be prepended to this quick list as well, as is the case for all credential generation strategies. Approximately 20 credentials are generated for all services to be bruteforced. ***Defaults Only*** Defaults only tries a small number of known default and common default passwords. Default only mode generates: • 16 credentials for postgres • 29 credentials for db2 • 141 credentials for ssh • 141 credentials for telnet • 22 credentials for mssql • 150 credentials for http • 4 credentials for https • 13 credentials for smb • 21 credentials for ftp ***Normal***

Setting Name	Description
	Normal tries a fixed maximum number of credentials. Expect it to take ~5 min / host on a fast LAN. The strategy focuses on common usernames (which are protocol-specific) as well as discovered usernames and many passwords (which are drawn from lists of common passwords). Most protocols also have common defaults, which are tried after known good credentials on other services/instances. Normal mode generates: • 4000 credentials for postgres • 3000 credentials for db2 • 10000 credentials for mysql • 1000 credentials for ssh • 1000 credentials for telnet • 10000 credentials for mssql • 6000 credentials for http • 1000 credentials for https • 4000 credentials for smb • 1000 credentials for ftp These generated credentials are tried after the current known good credentials, so it's common to see these credential figures adjusted on each successive run (assuming credentials become known as modules run). ***Deep*** Deep is identical to Normal, except three times more passwords are attempted. Expect it to take ~15-20 min / host on a fast lan, if all services are enabled. These extra passwords also come from the common password list. For the few protocols that support fast enough guesses, passwords are subjected to a fixed set of transformations (1 or I, 0 for O, etc). Deep mode generates: • 12000 credentials for postgres:5432 • 9000 credentials for db2:50000 • 30000 credentials for mysql:3306

Setting Name	Description
	• 132 credentials for ssh:22 • 132 credentials for telnet:23 (linux) • 30000 credentials for mssql:13013 • 18000 credentials for http:8080 (tomcat) • 3000 credentials for smb:445 (microsoft) **Note:** SSH and Telnet are not subject to the "deep" multiplier, as these credentials take too long to test compared to the other services. ***Known*** Known only tries credentials that are already known; these credentials are known as good (previously discovered, or supplied) for all services in the target workspace. This includes SSH keys in addition to passwords
Bruteforce Speed	• **Insane** should only be used on a fast LAN. • **Aggressive** works well for scans across most LANs. • **Normal** is recommended for external use. • **Polite** is useful across slow WAN links or to hide the scan. • **Sneaky** is very stealthy but requires some time. • **Paranoid** requires the most amount of time to complete.

Automated Exploitation Settings

The following table provides information for the settings that are available for automated exploitation.

Table 5: Automated Exploitation Settings

Setting Name	Description
Target Addresses	The addresses in scope for this exploit session.
Excluded Addresses	These are all IP addresses that will not be tested. If the IP has not been included in the ‘Target Addresses’ box, it does not need to be specifically excluded.
Minimum Reliability	All exploits have a rank assigned, based on its impact to the target system and the reliability of the exploit method. These rankings are found in the Reliability setting for exploits. • **Excellent** means the exploit will never crash the service.

Setting Name	Description
	Exploits with this ranking include SQL Injection, CMD execution, and certain weak service configurations. Most web application flaws fall into this category. • **Great** is the ranking for exploits that have a default target and either auto-detect the appropriate target, or use an application-specific return address after running a version check. These can crash the target, but are considered the mostly likely to succeed. • **Good** means the exploit has a default target and it is the common case for this type of software (English, Windows XP for a desktop app, 2003 for server, etc. • **Normal** indicates that the exploit is otherwise reliable, but depends on a specific version and can't reliably auto-detect. • **Average** ranked exploits are difficult to reliably leverage against some systems. • **Low** means the exploit fails more than 50% of the time for common platforms. • Manual exploits are so unstable or difficult to exploit and are basically a DoS. This ranking is also used when the module has no use unless specifically configured by the user (php_eval).
Concurrent Exploits	This is the number of simultaneous exploit attempts that will be run. The best number will vary based upon available CPU horsepower. Utilizing only one concurrent attempt will enable you to debug with the task log if issues are experienced.
Timeout in Minutes	This is the number of minutes that Express will wait for a given exploit. The default is set to ensure all exploits have sufficient time to complete, but you may need to increase this if target hosts are slow.
Connection Type	The connection type determines the method in which the payload connection is made: There are three connection types: auto, reverse, and bind.
Only Obtain One Session Per Target	This option allows you to only open one session per target and bypass any targets that already have a session open.
Ignore Known-Fragile Devices	This option allows you to bypass any known-fragile devices.
Skip Exploits that Do Not Match the Host OS	This option allows you to bypass any exploits that do not apply to the target OS.

Setting Name	Description
Run Payloads	Valid authentication credentials from the previous step should lead to the remote execution of a Metasploit payload, if possible. For SMB, this is psexec; for MSQQL this is mssql_payload, etc.
Transport Evasion	This option enables you to send small TCP packets and insert delays between them. **Low** – Inserts a delay of between 1-10 seconds between TCP packets. The delay rate will be constant for a specific module, but will vary across multiple modules. **Medium** – Transmits small TCP packets; payloads are fragmented into 15 byte payloads. **High** – Combines the Low and Medium settings by transmitting small TCP packets and inserting delays between them.
Application Evasion	This option enables you to define application-specific evasion options for DCERPC, SMB, and HTTP-based exploits. These are the only protocols that support evasions. Please note that not all protocols support all levels of evasion. **DCERPC** **Low** – Adds fake UUIDs before and after the actual UUID targeted by the exploit. **High** – Sets the maximum fragmentation size of DCERPC calls to a value between 4 and 64. **SMB** **Low** – Obscures the PIPE string, places extra padding between SMB headers and data, and obscures path names. **Medium** – Segments SMB read/write operations. **High** – Sets the max size for SMB reads and writes to 4-64 bytes. **HTTP (Client-Server Attacks Only)** **Low** – Adds "header folding," which splits HTTP headers into separate lines joined by whitespace by the server, and adds random cases to HTTP methods. This option adds between 1-64 fake HTTP headers. **Medium** – Adds 1-64 fake query strings to get requests. Adds 1-64 whitespace characters between tokens. Adds 1-64 POST parameters. **High** – Encodes some characters as percent-u unicoded characters (half, randomly), adds a fake "end" to HTTP requests before the attack, and uses backslashes instead of forward slashes.
Listener Ports	Defines the range of ports that will be used for reverse connect payloads.

Setting Name	Description
Listener Host	Defines the IP address for the payload to connect back to in cases where the address needs to be overridden.

Manual Exploitation Module Settings

The following table provides information for the settings that are available for manual exploitation.

Table 6: Manual Exploitation Module Settings

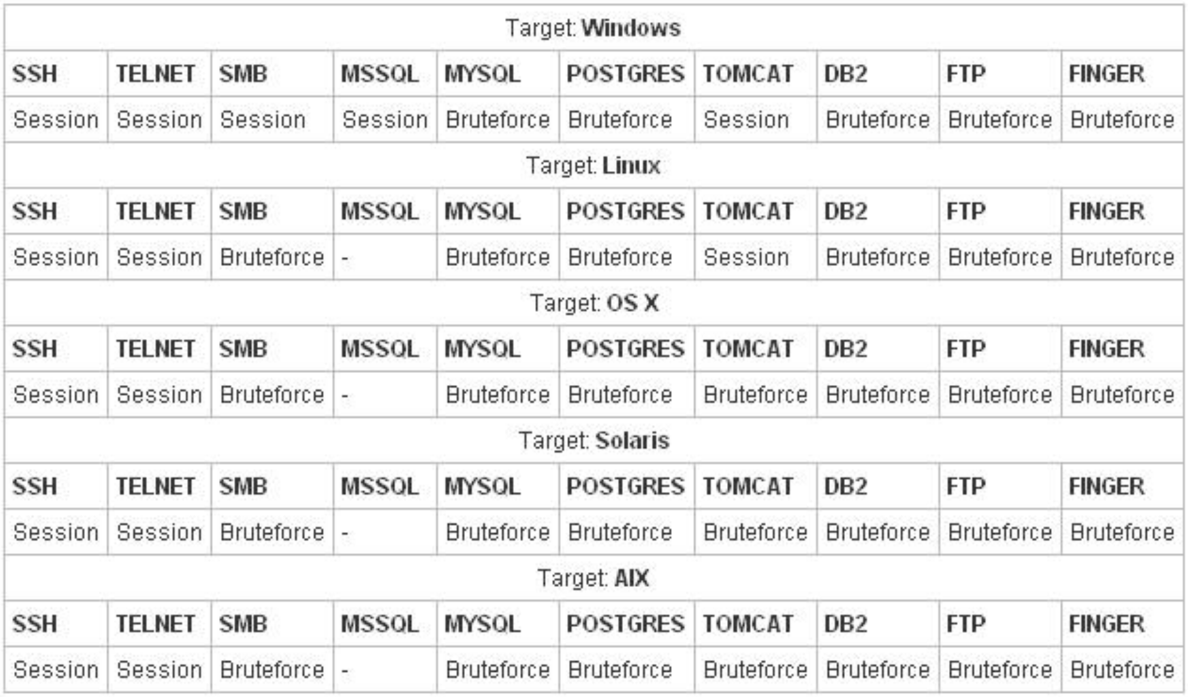
Setting Name	Description
Module Options	• **SRVHOST** – This refers to the address on which the local host will listen. • **SRVPORT** – This refers to the port on which the local port will listen. • **SSL** – Select this option to enable SSL negotiations for incoming SSL connections. • **SSL Version** – This refers to the version of SSL that will be used. SSL1, SSL2, and SSL3 are supported. • **URIPATH** – This refers to the URI that will be used for the exploit. By default, this value is random.
Excluded Addresses	These are all IP addresses that will not be tested. If the IP has not been included in the 'Target Addresses' box, it does not need to be specifically excluded.
Advanced Options	• **ContextInformationFile** – This refers to the information file that holds the context information. • **DisablePayloadHandler** – Select this option to disable the handler code for the selected payload. • **DynamicSehRecord** – Select this option to generate a dynamic SEH record. • **EnableContextEncoding** – Select this option to use transient context when payloads are being encoded.
Evasion Options	Evasion options will vary from module to module, depending on the type of exploit used. However, descriptions for each of evasion option will be provided next to the option name.

Supported Targets

The following section details the bruteforce and exploitation capabilities of Metasploit Express.

Bruteforce Targets

Use the following chart to determine the bruteforce capabilities of Metasploit Express. See the key below for descriptions of bruteforce, session, and untested.



Target: **Windows**									
SSH	**TELNET**	**SMB**	**MSSQL**	**MYSQL**	**POSTGRES**	**TOMCAT**	**DB2**	**FTP**	**FINGER**
Session	Session	Session	Session	Bruteforce	Bruteforce	Session	Bruteforce	Bruteforce	Bruteforce
Target: **Linux**									
SSH	**TELNET**	**SMB**	**MSSQL**	**MYSQL**	**POSTGRES**	**TOMCAT**	**DB2**	**FTP**	**FINGER**
Session	Session	Bruteforce	-	Bruteforce	Bruteforce	Session	Bruteforce	Bruteforce	Bruteforce
Target: **OS X**									
SSH	**TELNET**	**SMB**	**MSSQL**	**MYSQL**	**POSTGRES**	**TOMCAT**	**DB2**	**FTP**	**FINGER**
Session	Session	Bruteforce	-	Bruteforce	Bruteforce	Bruteforce	Bruteforce	Bruteforce	Bruteforce
Target: **Solaris**									
SSH	**TELNET**	**SMB**	**MSSQL**	**MYSQL**	**POSTGRES**	**TOMCAT**	**DB2**	**FTP**	**FINGER**
Session	Session	Bruteforce	-	Bruteforce	Bruteforce	Bruteforce	Bruteforce	Bruteforce	Bruteforce
Target: **AIX**									
SSH	**TELNET**	**SMB**	**MSSQL**	**MYSQL**	**POSTGRES**	**TOMCAT**	**DB2**	**FTP**	**FINGER**
Session	Session	Bruteforce	-	Bruteforce	Bruteforce	Bruteforce	Bruteforce	Bruteforce	Bruteforce

Figure 24: Bruteforce capabilities

- **Bruteforce** – Metasploit Express can identify valid credentials on the target.
- **Session** – Metasploit Express can gain code-execution and a session on the target. By definition, valid credentials are identified and recorded during this process.
- **Untested** – Denotes that untested platforms are likely to work, but have not been extensively tested.

Exploit Targets

Metasploit Express targets have been categorized into four tiers. This is the current state of the project at this time, and is subject to change:

- Windows (Tier 1 Platform) - Multitude of Exploits available. 0day regularly released. Meterpreter Support. New exploitation research is regularly integrated.
- UNIX (Tier 2 Platform) - Many Exploits available. Some Payloads / Shellcode available.

- Solaris (Tier 3 Platform) - Some Exploits available. Few Payloads / Shellcode available.
- OS X (Tier 3 Platform) - Some Exploits available. Few Payloads / Shellcode available.
- BSD, AIX, HPUX, Netware (Tier 4 Platform) - Few Exploits available. Payloads/ Shellcode may not be available.

Warnings

Before installing Metasploit Express, please read the following information:

- Antivirus (AV) software such as McAfee, Symantec, and AVG will cause problems with installation and at run-time. You **MUST** disable your AV before installing and using Metasploit Express.
- Local firewalls, including the Windows Firewall, **MUST** be disabled in order to run exploits successfully. Alternatively, the "bind" connection type may be used, but some exploits still need to receive connections from the target host.
- The RPC service (:50505) on Metasploit Express runs as ROOT, so any Metasploit Express account has privileged access to the system on which it runs. In malicious hands, this can lead to system or network damage. Please protect the service accordingly.
- Metasploit Express is intended only for authorized users. Run Metasploit Express only on machines you own or have permission to test. Using this software for criminal activity is illegal and could result in jail time.
- Local firewalls, including the Windows Firewall, will need to be disabled in order to run exploits successfully. Alternatively, the "bind" connection type may be used, but some exploits still need to receive connections from the target host.

Index