metasploit® pro

# Passive Network Discovery

## Quick Start Guide

In situations where active scanning causes instability in the target network, you can run a passive network scan to avoid detection and reduce disruptions. A passive network scan stealthily monitors broadcast traffic to identify the IP addresses of hosts on the network.  By initially running a passive scan, you can identify known hosts while evading network monitoring tools, such as intrusion detection systems (IDS). The data obtained from a passive network scan can be used to perform a targeted active scan with Metasploit's Discovery Scan.

The Passive Network Discovery MetaModule runs a live packet capture on a specific network interface to capture DHCP requests and ARP requests. If you want to have more granular control over the packet capture or you want to reduce the size of the packet capture, you can use Berkeley Packet Filters (BPF) to specify the types of packets that the MetaModule captures.

The packet capture runs until it reaches the maximum Pcap file size or the time limit you have configured for the MetaModule. When the MetaModule run completes, it stores the captured data and generates a comprehensive report of its findings.

## Product Terms

| | |
|---|---|
| **Berkeley Packet Filter (BPF)** | A packet filter that provides a raw interface to the data link layer and enables a very granular level of packet filtering. |
| **Packet Capture (Pcap)** | A  process that makes copies of packets off the wire. |
| **MetaModule** | A feature that extends the capabilities of modules in Metasploit Pro to perform penetration testing tasks. |
| **Notification Center** | A notification system that displays alerts for Metasploit tasks, MetaModules, and software updates. |

## Before You Begin

| | |
|---|---|
| **Use the Analysis Port** | To ensure that Metasploit Pro can monitor all network traffic, you should connect your Metasploit server to an analysis port on a network switch that has port mirroring enabled. Otherwise, you will only be able to capture traffic that is sent to and from the Metasploit server. |
| **Clear Your Browser's Cache** | After you install or update Metasploit, you must clear your browser's cache to ensure that all user interface elements load properly. |

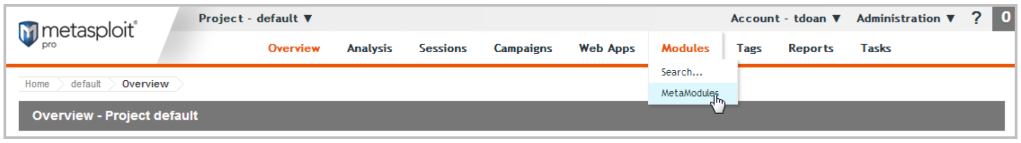
## Passive Network Discovery Scan

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

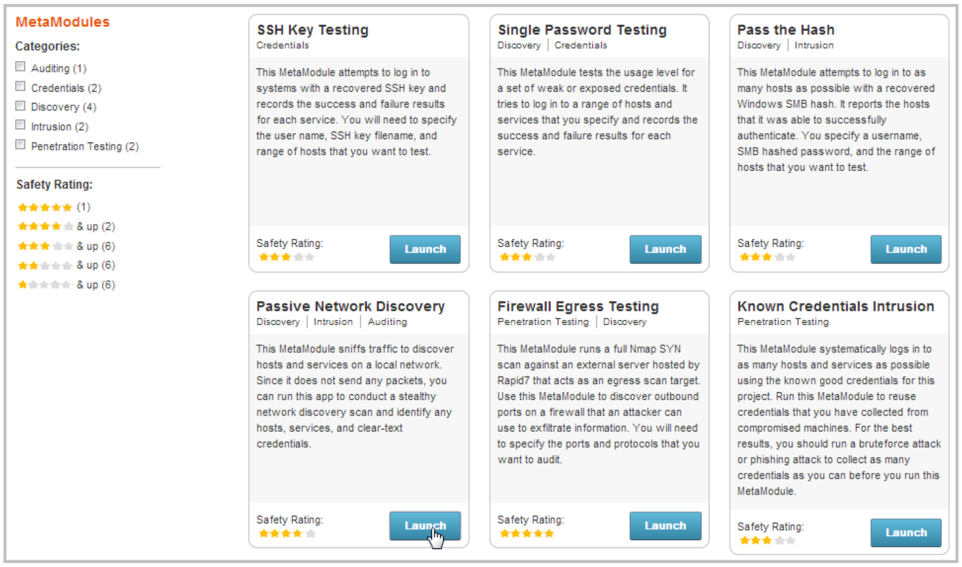
2. Open the default project.

Last updated 06/24/2013 - 4.7

3. Select **Modules > MetaModules**.



4. Find the **Passive Network Discovery** MetaModule and click the **Launch** button. The **Passive Network Discovery** window appears.


MetaModules

Categories:

- □ Auditing (1)
- □ Credentials (2)
- □ Discovery (4)
- □ Intrusion (2)
- □ Penetration Testing (2)

Safety Rating:

- ★★★★★ (1)
- ★★★★☆ & up (2)
- ★★★☆☆ & up (6)
- ★★☆☆☆ & up (6)
- ★☆☆☆☆ & up (6)

**SSH Key Testing**
Credentials

This MetaModule attempts to log in to systems with a recovered SSH key and records the success and failure results for each service. You will need to specify the user name, SSH key filename, and range of hosts that you want to test.

Safety Rating: ★★★☆☆ Launch

**Single Password Testing**
Discovery | Credentials

This MetaModule tests the usage level for a set of weak or exposed credentials. It tries to log in to a range of hosts and services that you specify and records the success and failure results for each service.

Safety Rating: ★★★☆☆ Launch

**Pass the Hash**
Discovery | Intrusion

This MetaModule attempts to log in to as many hosts as possible with a recovered Windows SMB hash. It reports the hosts that it was able to successfully authenticate. You specify a username, SMB hashed password, and the range of hosts that you want to test.

Safety Rating: ★★★☆☆ Launch

**Passive Network Discovery**
Discovery | Intrusion | Auditing

This MetaModule sniffs traffic to discover hosts and services on a local network. Since it does not send any packets, you can run this app to conduct a stealthy network discovery scan and identify any hosts, services, and clear-text credentials.

Safety Rating: ★★★★☆ Launch

**Firewall Egress Testing**
Penetration Testing | Discovery

This MetaModule runs a full Nmap SYN scan against an external server hosted by Rapid7 that acts as an egress scan target. Use this MetaModule to discover outbound ports on a firewall that an attacker can use to exfiltrate information. You will need to specify the ports and protocols that you want to audit.

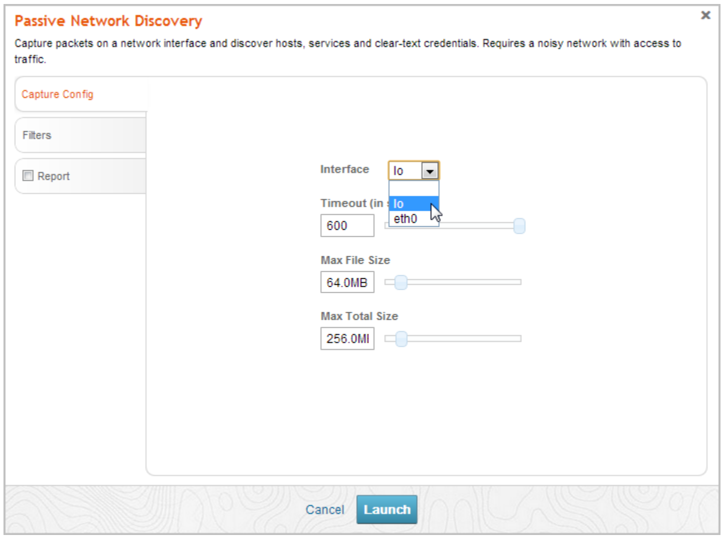
Safety Rating: ★★★★★ Launch

**Known Credentials Intrusion**
Penetration Testing

This MetaModule systematically logs in to as many hosts and services as possible using the known good credentials for this project. Run this MetaModule to reuse credentials that you have collected from compromised machines. For the best results, you should run a bruteforce attack or phishing attack to collect as many credentials as you can before you run this MetaModule.

Safety Rating: ★★★☆☆ Launch

5. From the **Pcap Configuration** tab, select the Network Interface Card (NIC) you want to use to capture traffic.  Metasploit automatically detects the interfaces that are available.


Passive Network Discovery ×

Capture packets on a network interface and discover hosts, services and clear-text credentials. Requires a noisy network with access to traffic.

Interface: lo

Timeout (in: 600

Max File Size: 64.0MB

Max Total Size: 256.0MI

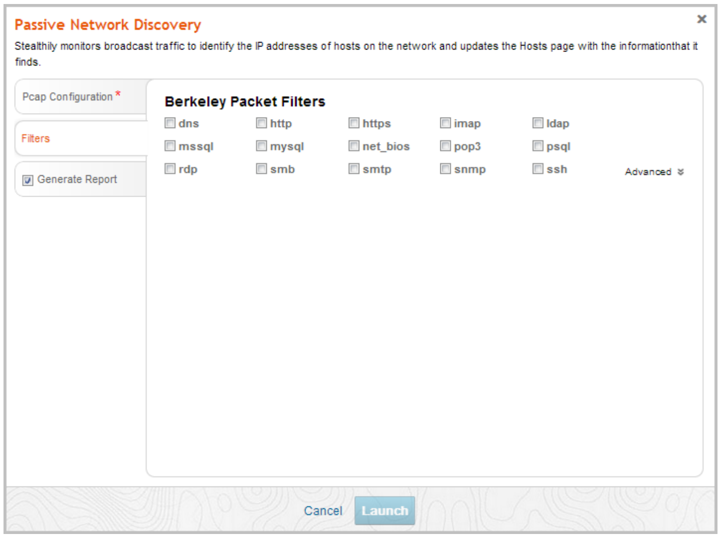
6. Define the limits you want to impose on the packet capture. You can use the sliders to define the following limits:

   - **Timeout** - The time limit for the capture, in seconds.
   - **Max File Size** - The maximum file size for each file captured, up to 512 MB.
   - **Max Total Size** - The maximum size of the entire Pcap file, up to 2GB. This value must be larger than the Max File Size.

   The packet capture runs until it meets the timeout limit or the maximum Pcap file size limit.

7. Click on the **Filters** tab.

8. Select the Berkeley Packet Filters that you want to use. For more information about BPFs, visit [http://biot.com/capstats/bpf.html](http://biot.com/capstats/bpf.html).



Passive Network Discovery

Stealthily monitors broadcast traffic to identify the IP addresses of hosts on the network and updates the Hosts page with the informationthat it finds.

Pcap Configuration *

Filters

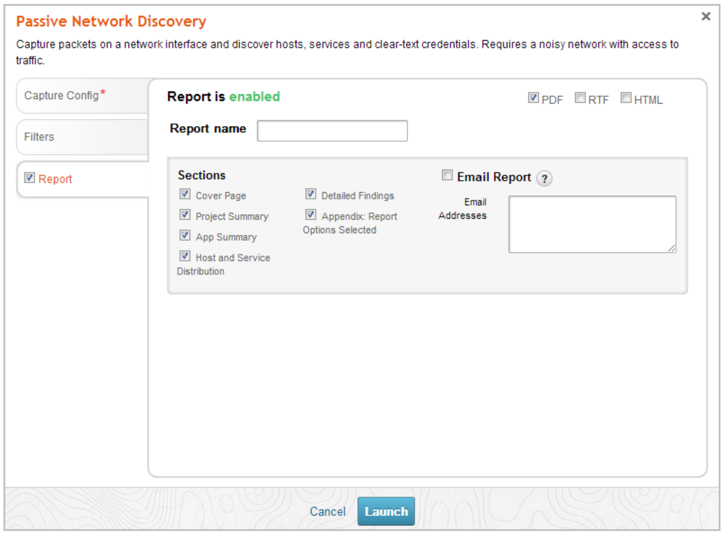
☑ Generate Report

Berkeley Packet Filters

□ dns □ http □ https □ imap □ ldap
□ mssql □ mysql □ net_bios □ pop3 □ psql
□ rdp □ smb □ smtp □ snmp □ ssh

9. Click the **Report** tab.

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



Passive Network Discovery

Capture packets on a network interface and discover hosts, services and clear-text credentials. Requires a noisy network with access to traffic.

Capture Config *

Filters

☑ Report

Report is enabled

☑ PDF □ RTF □ HTML

Report name

Sections

☑ Cover Page
☑ Project Summary
☑ App Summary
☑ Host and Service Distribution
☑ Detailed Findings
☑ Appendix: Report Options Selected

□ Email Report

Email Addresses

11. Select whether you want to generate the report in PDF, RTF, or HTML. PDF is the preferred format.

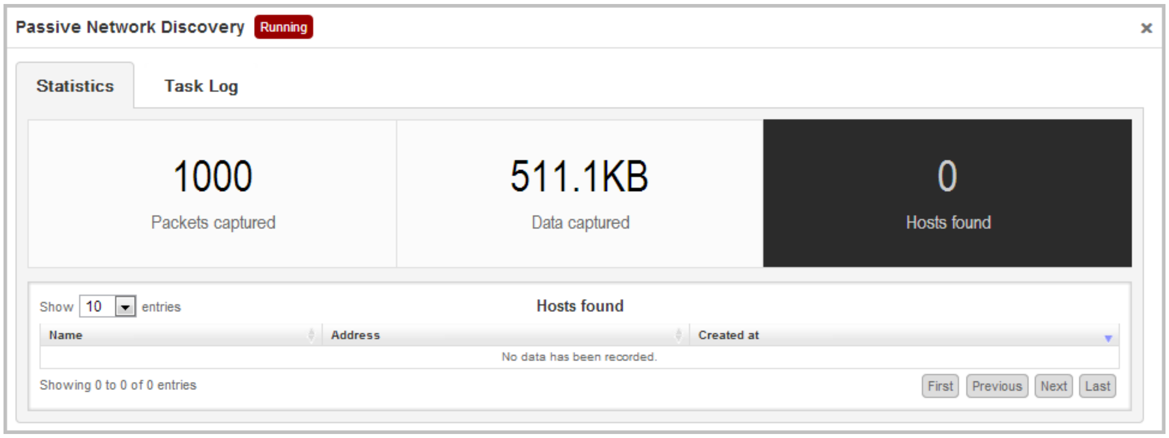
12. From the **Sections** area, deselect any sections you do not want to include in the report. Skip this step if you want to generate all the report sections.

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

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

14. Click the **Launch** button.

When the MetaModule launches, the Findings window appears. It contains the statistics and task log for the MetaModule run. You can track the total number of packets, bytes, and hosts that the MetaModule captures in real-time.



Passive Network Discovery Running

| 1000 | 511.1KB | 0 |
|---|---|---|
| Packets captured | Data captured | Hosts found |

Show 10 entries

Hosts found

| Name | Address | Created at |
|---|---|---|
| No data has been recorded. | | |

Showing 0 to 0 of 0 entries

After the MetaModule completes its run, you should go the Reports area to view the Passive Network Discovery Findings Report that the MetaModule generated. The report provides detailed information about the services and credentials that the MetaModule was able to capture for each host, as well as a graphical breakdown of the operating systems and services that were found.