metasploit®
pro

Segmentation and Firewall Testing

Tutorial

When firewalls have badly configured or lax egress traffic filtering policies, they open the network up to attacks from reverse shells, data-exfiltration, and other forms of exploitation. In order to identify the open ports that allow outbound traffic and to verify that your egress filtering policies properly block traffic, you can run the Segmentation and Firewall Testing MetaModule.

The MetaModule runs an Nmap SYN scan against an egress target to reveal the outbound ports that are open from an internal host. The egress target, `egadz.metasploit.com`, is a server hosted by Rapid7 and has been set up to have all 65,535 ports open. Each port is configured to respond with a single SYN-ACK packet. In its default configuration, the MetaModule initiates a port scan using Nmap's default 1,000 most common ports; however, if you need to include additional ports, you can define a custom port range.

When the MetaModule runs, it identifies the state of the ports in your firewall based on the traffic received by the egress target. If it receives the traffic, then the MetaModule flags the port as open. If the firewall blocks the traffic, the MetaModule flags the port as filtered. The MetaModule tags the remaining ports as unfiltered or closed depending on the their response to connections.

After the MetaModule completes its run, it generates a report that provides you with a comprehensive look at port state distribution and unfiltered ports.

Before You Begin

Turn off Wi-Fi	Before you run the Segmentation and Firewall Testing MetaModule, you must turn off your wireless internet connection. You should use your local area network to ensure that the MetaModule can reach the egress target.
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.

Product Terms

Data Exfiltration	A method of extracting data, such as simple file transfers that use netcat or ssh to perform a secure copy.
Egress Target	An external server, `egadz.metasploit.com,` hosted by Rapid7 that acts as an egress target.
Egress Traffic	Traffic that is initiated from an internal network to an external host.
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.

Last updated 07/17/2013 - 4.7

Port States

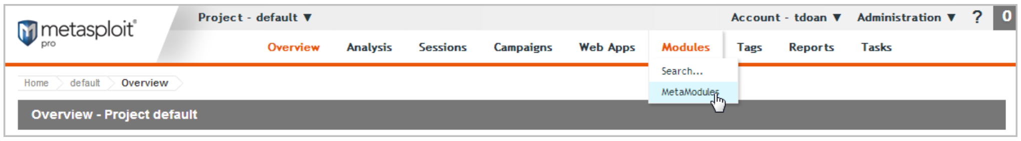
Open	A port is assigned an **open** state if it allows traffic out of the network and the egress target receives it.
Filtered	A port is assigned a **filtered** state if it drops the traffic before it reaches the desired port on the egress target.
Closed	A port is assigned a closed state if it allows traffic through the port, but there is not an application or service bound to the port.
Unfiltered	A port is assigned an **unfiltered** traffic if it allows traffic through to the port, but it cannot be determined whether the port is open or closed.

Segmentation and Firewall Testing

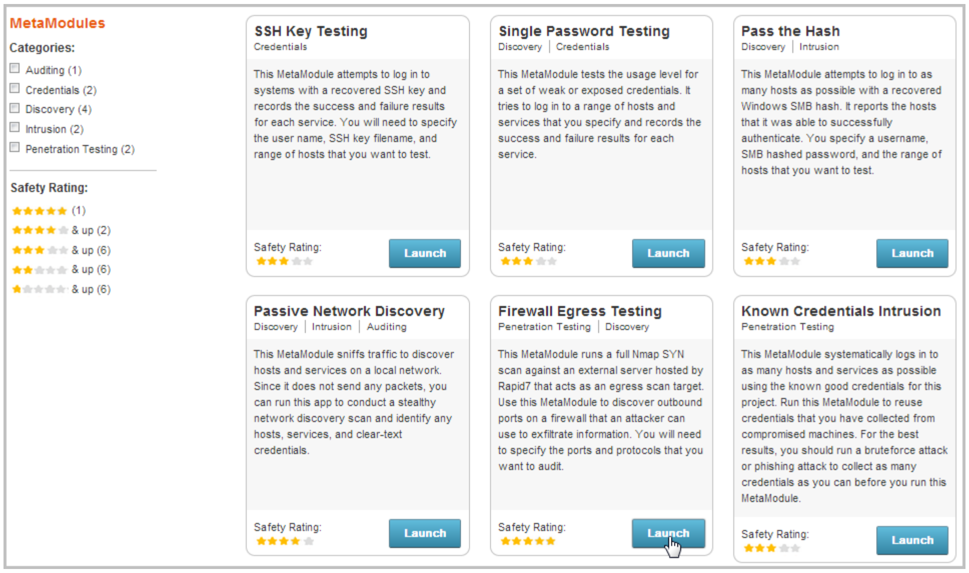
1. Log in to the Metasploit Pro web interface (https://localhost:3790).

2. Open the default project.

3. Select **Modules** > **MetaModules**.



4. Find the **Segmentation and Firewall Testing** MetaModule and click the **Launch** button. The **Segmentation and Firewall Testing** 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: ★★★☆☆

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: ★★★☆☆

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: ★★★☆☆

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: ★★★★☆

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: ★★★★★

Known Credentials Intrusion
Penetration Testing

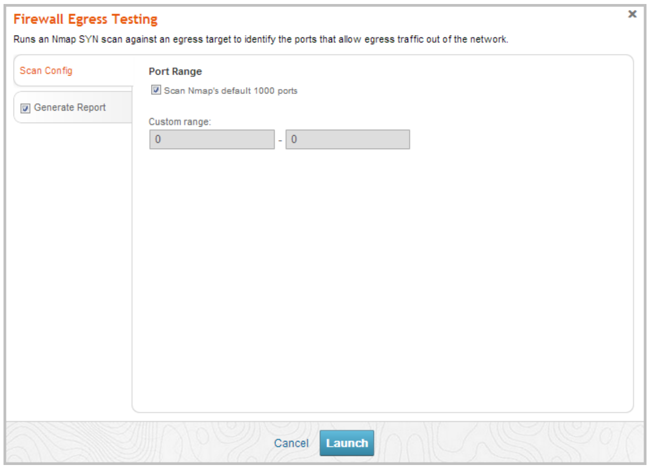
This MetaModule systematically logs in to as many hosts and services as possible using the known good credentials for this project. Run this MetaModule to reuse credentials that you have collected from compromised machines. For the best results, you should run a bruteforce attack or phishing attack to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

Safety Rating: ★★★☆☆

5. From the **Scan Configuration** tab, do one of the following:

   - If you want to scan Nmap's most common ports, leave the default settings.

   - If you want to create a custom port range, deselect the **Scan Nmap's default 1000 ports** option and enter the port range you want to scan in the **Custom Range** fields.



Firewall Egress Testing

Runs an Nmap SYN scan against an egress target to identify the ports that allow egress traffic out of the network.

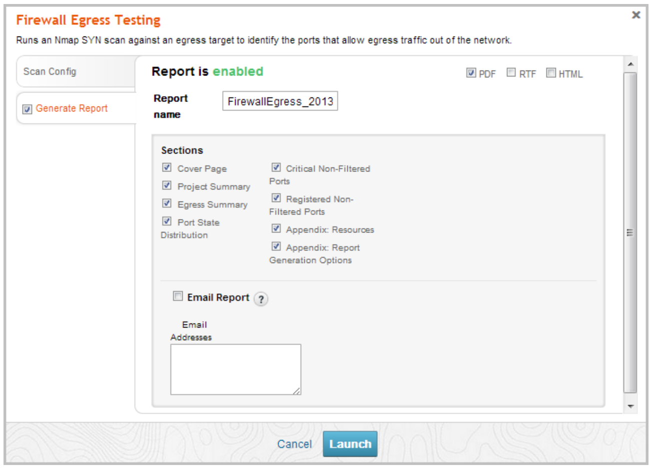
Port Range

☑ Scan Nmap's default 1000 ports

Custom range: 0 - 0

6. Click the **Report** tab.

7. 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.



Firewall Egress Testing

Runs an Nmap SYN scan against an egress target to identify the ports that allow egress traffic out of the network.

Report is enabled ☑ PDF ☐ RTF ☐ HTML

Report name: FirewallEgress_2013

Sections

☑ Cover Page
☑ Project Summary
☑ Egress Summary
☑ Port State Distribution
☑ Critical Non-Filtered Ports
☑ Registered Non-Filtered Ports
☑ Appendix: Resources
☑ Appendix: Report Generation Options

☐ Email Report

Email Addresses

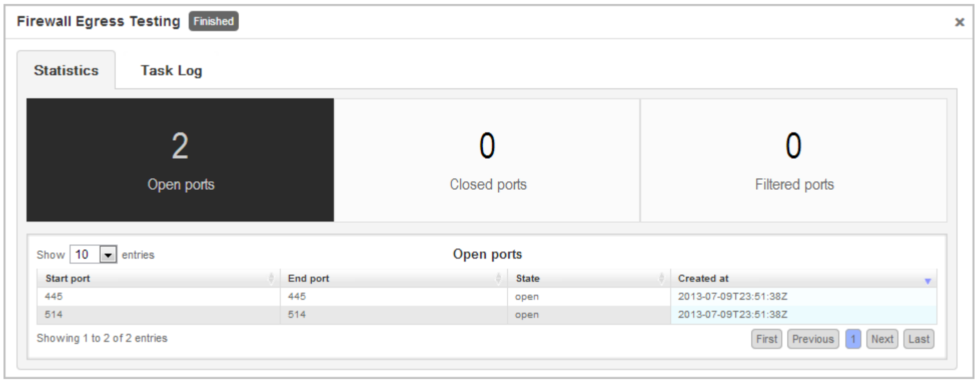
8. From the **Sections** area, deselect any sections you do not want to include in the report. Skip this step if you want to generate all the report sections.

9. 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 mail server settings, select **Administration** > **Global Settings** > **SMTP Settings**.

10. Click the **Launch** button.

When the MetaModule launches, the Findings window appears and displays the real-time statistics and tasks log for the MetaModule run. You can track the total number of open, flitered, and closed ports that the MetaModule identifies from the Statistics tab. If you want to view all the event details, you can click on the Task Log tab.



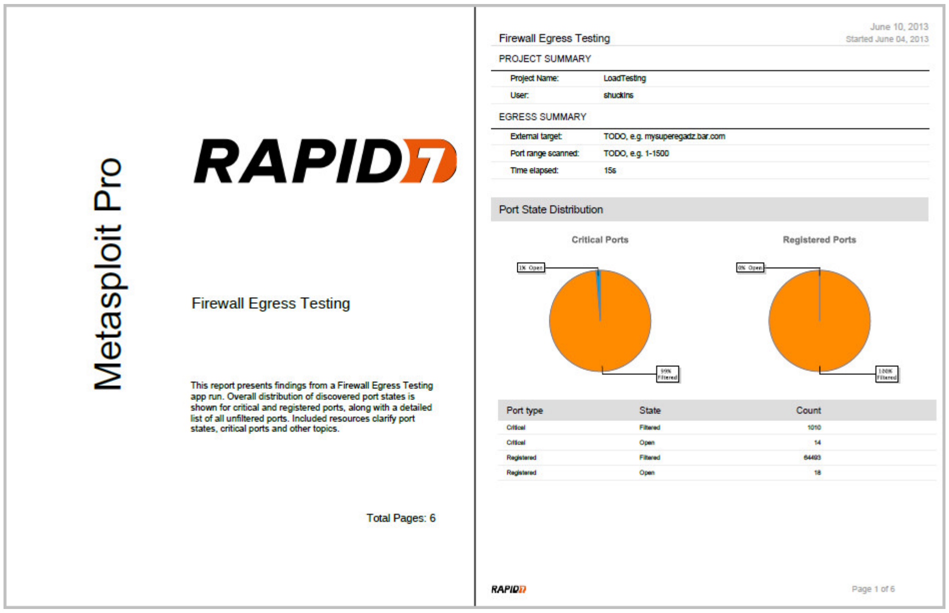
2	0	0
Open ports	Closed ports	Filtered ports

Open ports

Start port	End port	State	Created at
445	445	open	2013-07-09T23:51:38Z
514	514	open	2013-07-09T23:51:38Z

Showing 1 to 2 of 2 entries

After the MetaModule completes its run, you should go the Reports area to view the Segmentation and Firewall Testing Report. You can compare the results to your firewall filtering policies. The Critical Non-filtered Ports and Registered Non-filtered Ports section detail the ports that allowed traffic out of your network. You should review these ports and add filtering policies to address any ports should not allow outbound connections.



Metasploit Pro

RAPID7

Firewall Egress Testing

This report presents findings from a Firewall Egress Testing app run. Overall distribution of discovered port states is shown for critical and registered ports, along with a detailed list of all unfiltered ports. Included resources clarify port states, critical ports and other topics.

Total Pages: 6

Firewall Egress Testing

June 10, 2013
Started June 04, 2013

PROJECT SUMMARY

Project Name:	LoadTesting
User:	shuckins

EGRESS SUMMARY

External target:	TODO, e.g. mysuperegadz.bar.com
Port range scanned:	TODO, e.g. 1-1500
Time elapsed:	15s

Port State Distribution

Port type	State	Count
Critical	Filtered	1010
Critical	Open	14
Registered	Filtered	64493
Registered	Open	18

RAPID7

Page 1 of 6

The Segmentation and Firewall Testing MetaModule uses a server hosted by Rapid7 to determine what ports allow egress traffic out of a network. In some scenarios, you may want to set up your own egress testing server. This is useful when you want to test egress between different endpoints, or if you don't want to send data to a server on the internet.

Creating your own egress testing server is easy. All you need is a linux box loaded with your favorite distribution and configured with two IP addresses. The first IP address will be an admin interface. This is usually found on the eth0 interface. This IP will be used for controlling the egress testing server, usually via SSH. The second IP address will host the egress testing server. This is usually found on eth1, or a virtual interface such as eth0:1. This is the IP you will scan from the Metasploit Firewall Egress Testing MetaModule.

Egress testing is done by opening all ports on the egress testing IP. Please keep in mind that opening all ports can be a security risk. To limit per-connection resources, we use the TARPIT functionality built in to iptables to open all ports. Iptables tarpitting captures and holds incoming TCP connections using no local per-connection resources. Connections are accepted, but immediately switched to the persist state (0 byte window). This allows Metasploit to accurately determine open egress ports using SYN scans, while keeping others off your server.

First, ensure iptables tarpitting is installed:

```
# On debian based systems:
apt-get install xtables-addons-common
# On redhat based systems:
yum install xtables-addons
```

Next, create an iptables rule to tarpit all connections destined for your egress testing IP:

```
# Replace 10.254.254.254 with your egress testing IP:
iptables -I INPUT 1 -d 10.254.254.254/32 -p tcp -m tcp -j TARPIT --tarpit
```

That's it! You may (and probably should) configure iptables to accept SSH connections as well as drop all other connections. This can be done with these commands:

```
# Accept SSH connections
iptables -A INPUT -p tcp -m tcp --dport 22 -j ACCEPT
# Drop all other connections
iptables -P INPUT DROP
```

Armed with your own egress testing server, use the advanced options of the Metasploit Firewall Testing MetaModule to scan your IP.