

Lab Report

Your Performance

Your Score: 4 of 4 (100%)

Elapsed Time: 4 minutes 45 seconds

Pass Status: Pass

Required Score: 100%

Task Summary

- ✓ Enable IPS [Show Details](#)
- ✓ Update signature manually with SBIPS000018.bin
- ✓ Set to update signature automatically [Hide Details](#)

- ✚ Automatically Update Signatures selected
 - ✚ User Name: mary.r.brown
 - ✚ Password: Upd@teN0w

- ✓ Set IPS Policies to Detect and Prevent [Hide Details](#)

- ✚ Set Backdoor to Detect and Prevent
 - ✚ Set DOS to Detect and Prevent
 - ✚ Set Exploit to Detect and Prevent
 - ✚ Set FTP to Detect and Prevent
 - ✚ Set LDAP to Detect and Prevent
 - ✚ Set Shellcode to Detect and Prevent
 - ✚ Set SQL-DB to Detect and Prevent
 - ✚ Set TrojanVirus to Detect and Prevent
 - ✚ Set WebServer to Detect and Prevent

Explanation

In this lab, you perform the following:

- Enable the IPS on the LAN and DMZ interface.
- Manually update the IPS signature using **C:\signatures\sbips000018.bin**
- Configure the NSA to automatically update the signature in the future.
 - User name: **mary.r.brown**
 - Password: **Upd@teN0w** (0 is zero)
- Set the IPS policy to detect and prevent all known threats.

Complete this lab as follows:

1. Enable the IPS as follows:
 - a. In the Security Appliance Configuration utility, select **IPS**.
 - b. Under IPS Enable, select **Enable IPS Protection for LAN**.
 - c. Select **Enable IPS Protection for DMZ**, and then click **Apply**.
2. Update the IPS signature as follows:
 - a. Under Manual Signature Updates, select **Browse**.
 - b. Browse to and select **C:\Signatures\SBIPS000018.bin**.
 - c. Click **Open**.
 - d. Select **Upload**.
 - e. Refresh the page to update the IPS Signatures status.
 - f. Select **Automatically Update Signatures**.

- g. Enter the *user name*.
 - h. Enter the *password*; then click **Apply**.
3. Configure IPS Policy as follows:
- a. In the left menu, select **IPS Policy**.
 - b. Select **Detect and Prevent** for each IPS Category.
 - c. Click **Apply**.