ICT2203 Network Security
2021-2022 Trimester 3

Laboratory 6.2:
Attacks and Defense of IP Networks with Firewalls (II)

LEARNING OUTCOMES

Upon completion of this laboratory exercise, you should be able to:

- Conduct Cross Scripting Attack using DVWA (Damn Vulnerable Web Application).
- Configure ASA to inspect HTTP application layer protocol and use the same to defend against XSS.

REQUIRED HARDWARE

- 1 x Rack of Cisco network devices
- 1 x Box of Ethernet and console cables
- 3 x Laptops

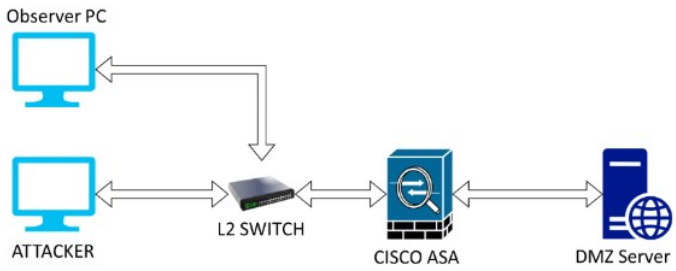
REQUIRED SOFTWARE

- Tera Term 4.105 http://ttssh2.osdn.jp/index.html.en
- Damn Vulnerable Web Application

EXERCISE 1: CONDUCT CROSS SCRIPTING ATTACK (XSS) USING DVWA

1.1: Downloading DVWA Files

1.1.1 Setup the network topology as shown below:



1.1.2 Configure appropriate security levels and make sure that the Attacker and Observer PC can access the XAMPP server launched on the "DMZ SERVER"

1.1.3 Download the DVWA files using the following link on the "DMZ SERVER": https://github.com/digininja/DVWA/archive/master.zip

1.1.4 Go to the folder C:\xampp\htdocs and create a new folder with the name "DVWA"

1.1.5 Unzip the downloaded DVWA master files. Copy the contents of this file and place them in the created "DVWA" folder. See Figure 1 for details.

1.1.6 Go to folder C:\xampp\htdocs\DVWA\config and change the name of the file "config.inc.php.dist" to "config.inc.php"

1.1.7 Right click on the file "config.inc.php" and select edit with notepad++. Once the file opens, edit the following data and save the file.

$_DVWA['db_user'] = 'root';
$_DVWA['db_password'] = '(empty)'; (leave it empty)

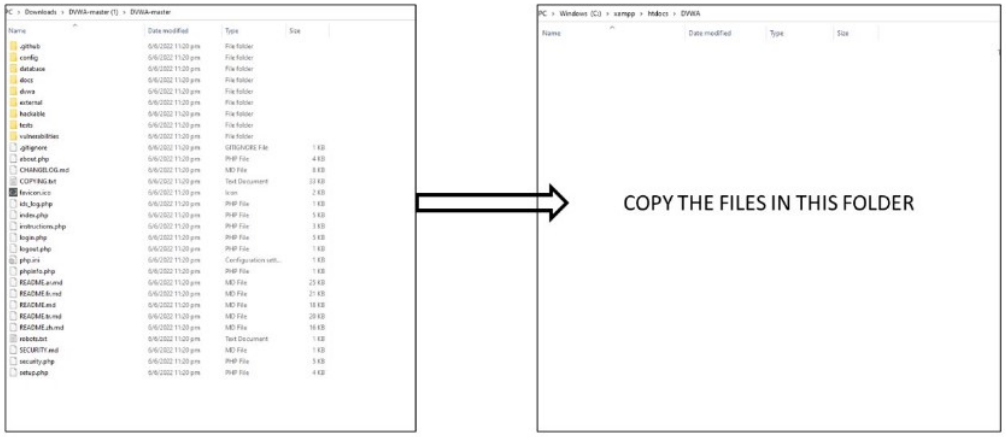


Figure 1: Copying DVWA Files

1.2: Implement XSS Attack using DVWA

1.2.1 Launch the DVWA application on all the PCs. To launch, open any browser and go to "server_address"/dvwa.

1.2.2 Click on "Create Database" and then click on "Login". Input the user as "admin" and password as "password".

1.2.3 On the Attacker PC click on "XSS (Stored)" on the left side panel. Type anything under "Name". Under message type the following:

<script>alert("What is Happening");</script>

1.2.4 Click on "Sign Guestbook" and observe the output. Now go to the Observer PC and repeat steps 1.2.1 and 1.2.2. Click on "XSS (Stored)" and observe the output.

1.2.5 Instead of typing the message referred to in 1.2.3, type the following and observe what happens:

<script>window.location = https://www.google.com;</script>

1.3: Configuring ASA to inspect HTTP application

1.3.1 As discussed in the lecture, ASA is an application-aware staeful firewall which can also perform application layer inspection.

1.3.2 Thus, following the security principle of defense-in-depth, ASA should also assist to defend potential attacks on web servers instead of leaving the web servers to defend themselves.

1.3.3 Read through the lecture notes on the use of MPF to configure HTTP inspection policy map and devise a HTTP inspection policy map to block urls with the term “vulnerabilities” in it.

1.3.4 When ready, configure your HTTP inspection policy map in the ASA.

1.3.5 Remember to also configure MPF layer 3/4 class map and policy map to apply your HTTP inspection policy map, and then activate it on appropriate ASA interface.

1.3.6 When done, check if you can implement step 1.2.3. If you can implement, then you have not configured the policy correctly.

1.3.7 Another way to defend is to check for the word “script” in the text. Devise an approprtiate inspection policy map accordingly and check if you can defend against the specific attacks in 1.2.3 and 1.2.5.