NettechCloud
A Passion to See You at the Top

Lab1: Building your own Lab

Lab Objective:

- Preparing VMware Workstation
- Deploying F5 BIGIP System in Virtual Environment
- Licensing and Resource Provisioning
- Network configuration

To deploy BIG-IP Virtual Edition on your workstation, VMware provides two great solutions:

- VMware Fusion
- VMware Workstation
  (For this Lab guide, we'll use VMware Workstation)

Step1: Preparing VMware

VMware is the virtual environment that will host F5 BIGIP System. We need to prepare it in the right way to make this setup work. The virtual machine **[F5 BIGIP VE]** comes with **four virtual NICs**, but we are going to use only three of them. The first one is the out-of-band management, and you need to configure there the IP address you wish to manage your F5 on. All the other interfaces will actively send traffic, and you can tune them at will. Just note that the management interface must be on a separate network than the production interfaces.

Net Adapter	Vmnet1, host only	Management	172.16.1.0/24	Mgmt. Port
Net Adapter 2	Vmnet2, host only	Internal	10.128.1.0/24	1.1
Net Adapter 3	Vmnet3, host only	External	192.168.200.0/24	1.2

Lab4: Web Application Vulnerabilities

Objective:

- Demonstrate Parameter Tampering
- Demonstrate Hidden Field Manipulation
- Demonstrate SQL injection

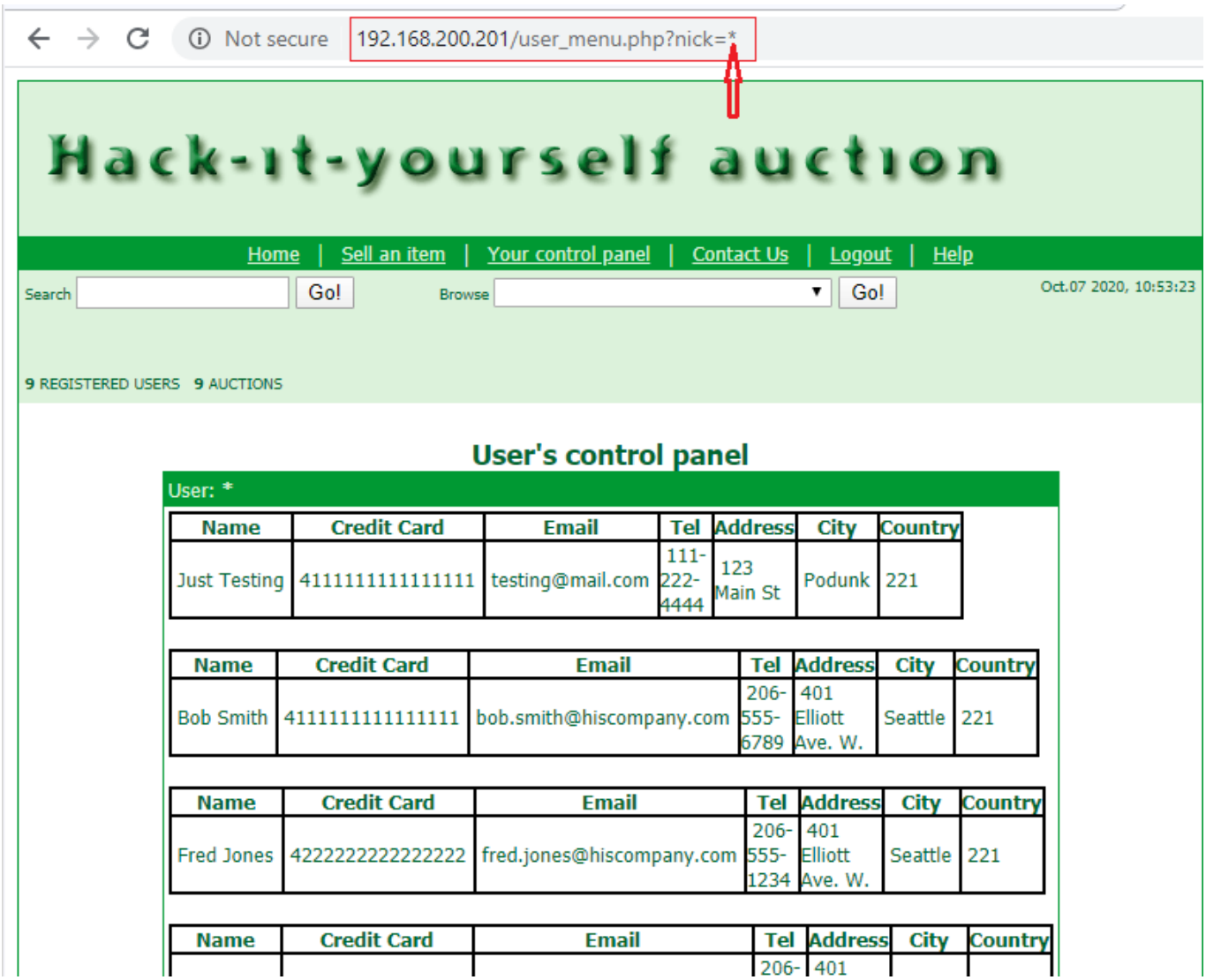
Lab Requirements:

. Client machine has access to the auction site and associated virtual server

. Client machine has Fiddler software installed

Exercise 1: Parameter Tampering

1. Open a new browser session on your PC and connect to the auction site represented by your virtual server **(http://192.168.200.201/index.php)**
2. In the user login section of the auction site, enter **student1** username and **nettech1** password
3. Click **Go!.**
4. Click the **control panel** link located below your username you will see your personal credentials.
5. In the browser address field, replace the URI value of **student1** with another student.(student2, student3, etc.) as shown in this example. **http://192.168.200.201/user_menu.php?nick=**student2
6. Can you view that student's personal credentials?
7. Now replace the value of 'nick with **"*"**.



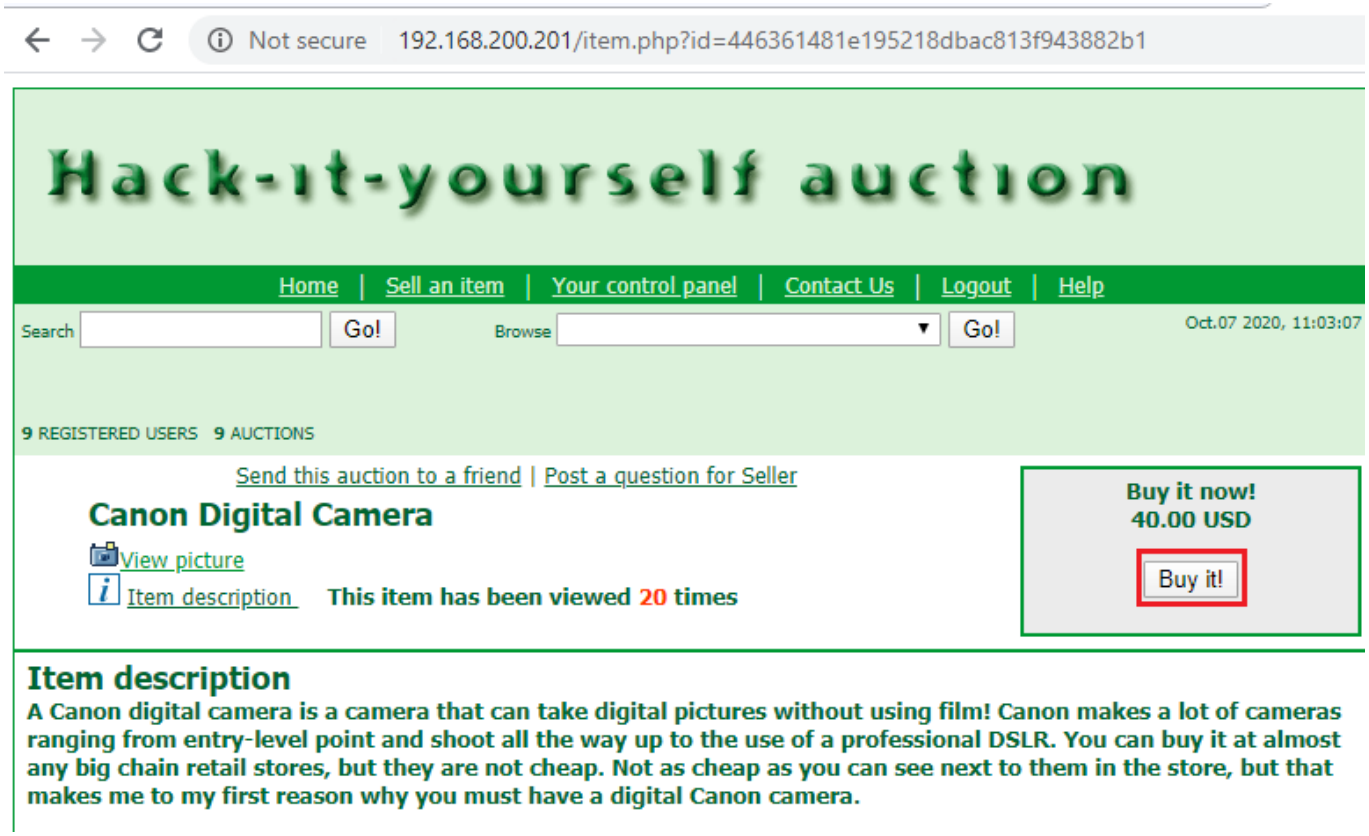
All users should now appear. This happens because the asterisk is a wildcard in many versions of SQL. In this case, it selects everything from the user_menu table in hack-it because it is passed directly to the back end.

Exercise 2: Hidden Field Manipulation

8. Click on the **Home** link at the top of the auction site.
9. Click on one of the items in the last created auctions section.
10. Start **Fiddler**.
11. Click on **rules**, then select **Automatic Breakpoints**, and then choose Before Request F11.

Note- The automatic Breakpoints option in Fiddler will stop network traffic in order for you to modify request on the fly.

12. Return to the auction site, and then click **buy it**!



13. Navigate Back to **Fiddler**.
14. Click on the Web session that contains the **/buy.php** URL.
15. Click the **Inspectors** tab, and then click the **webForms** button below the tab.
16. Find and edit the **Price** value as desired.
17. Click **Run to Completion**.
18. Navigate back to the auction site and notice the Price value has changed to the value you chose.
19. Return to **Fiddler** and turn off Automatic ***breakpoints*** (shift-F11).
20. Exit Fiddler.

Exercise 3 : Cross Site Scripting (XSS)

21. We now want to sell an item. Go to **http://192.168.200.201/sell.php**
22. Complete the page for selling an item, using the using the following values:

	Auction Starts with	**Your choice**
	Duration	**Your choice**
	Country	**Your choice**
	Zip Code	**Your choice**
	Payment methods	**Your choice**
	Choose a category	**Your choice**
When complete, click		**Submit Query**

Lab 7: Creating a User-Defined Attack Signature

Lab Objective:

- Create a New Security Policy
- Create a user-defined attack signature
- Associate signature with signature set
- Apply signature set to security policy
- Trigger a violation and examine it
- Enforce an attack signature
- Change policy Enforcement Mode and test results

Lab Requirements

- Access to the auction site via a working Virtual server
- A working user account on the auction site

Expected Results

After completing this lab you should be able to trigger an attack signature violation based on a custom pattern that you create.

Create Security Policy based on Rapid Deployment template

1. In the Configuration Utility, Navigate to **Security>>Application Security>> Security Policies>>Policies List**
2. Click **Create New policy** and click on **Advanced** tab for advanced configuration
3. Configure the following settings for the new security policy:

Deployment Wizard		
Configure Security Policy Properties		
	Security Policy Name	**Lab7_attack_sig**
	Policy Type	**Security**
	Policy template	**Rapid Deployment Policy**
	Virtual Server	Do not associate with virtual Server option. We will manually assign this security policy to a virtual server
	Enforcement Mode	**Transparent**
	Application Language	**Unicode(utf-8)**
	Signature Staging	**Enabled**
	Enforcement Readiness Period	**7days**
When complete, click....		**Next**

Ensure that **signature staging** is enabled (the default setting). This means that attack signatures will be applied to requests. It also means that no request will be blocked if they trigger a violation because of an attack signature- even if the

A

1. Go to **Local Traffic>> Virtual Servers: Virtual Server List**.

Lab 9: Cookie Tampering

Lab Objectives:

- Learn cookie by sending a cookie header and value
- Tamper with cookie in order to trigger a violation.

Lab Requirements:

- Access to the auction site via a working virtual server with Application security policy enabled
- A working user account on the auction site
- A working security Policy created using the manual method
- Access to the Fiddler HTTP Proxy

Create a security Policy

1. In the Configuration Utility, Navigate to **Security>>Application Security>> Security Policies>>Policies List**
2. Click **Create New policy** and click on **Advanced** tab for advanced configuration
3. Configure the following settings for the new security policy:

Deployment Wizard		
Configure Security Policy Properties		
	Security Policy Name	**Lab9_cookie**
	Policy Type	**Security**
	Policy template	**Rapid Deployment Policy**
	Virtual Server	**Auction_VS1**
	Enforcement Mode	**Transparent**
	Application Language	**Unicode(utf-8)**
	Server Technologies	**Apache Tomcat** **MySQL** **PHP** **Unix/Linux**

Lab 13: Automatic Policy Building

Lab Objectives:

- Configure a policy using the automatic method
- Verify automatic security policy modification
- Differentiate between Fundamental and Comprehensive Policy types

Lab Requirements:

- Access to the Auction site via a working virtual server with Application Security policy enabled
- A working user account on the auction site.

Configure the security policy

1. In the Configuration Utility, Navigate to **Security>>Application Security>> Security Policies>>Policies List**
2. Click **Create New policy** and click on **Advanced** tab for advanced configuration

---

Note: This virtual server does not have a logging Profile assigned to it. You will add a logging profile in order to log all request, at the end of this Lab

---

3. Configure the following settings for the new security policy:

Deployment Wizard		
Configure Security Policy Properties		
	Security Policy Name	**Auto**
	Policy Type	**Security**
	Policy template	**Comprehensive**
	Virtual Server	**Auction_VS1**
	Enforcement Mode	**Blocking**
	Application Language	**Unicode(utf-8)**
	Server Technologies	**None**
	Signature Staging	**Enabled**
	Learning Mode	**Automatic**
When complete, click....		**Next**

4. Click **Create Policy**
   Your security Policy is now configured.

Assign a Log Profile to log all requests

Let's ensure that when we begin observing HTTP traffic to an Application security Policy associated with this virtual server, all request will be visible in the **Requests List.**

Examine Current Learning Scheme for Entities

1. Go to **Security>>Application Security: Policy building: Learning and blocking settings.**
2. Ensure you are viewing your automatic policy.
3. In the Policy Building Settings section, expand **File Types, URLs** and **Parameters**
4. What is the learning scheme? It should be Learn **"Always"**

Send requests before adding a trusted IP Address

5. Go to the auction site and sell an item. There are lots of parameter on the **sell**. **Php** page and you will see plenty of entries in the next step.
6. Go to the Traffic Learning screen. There should be learning suggestions for various parameters and file types, with learning scores around **5 percent**.

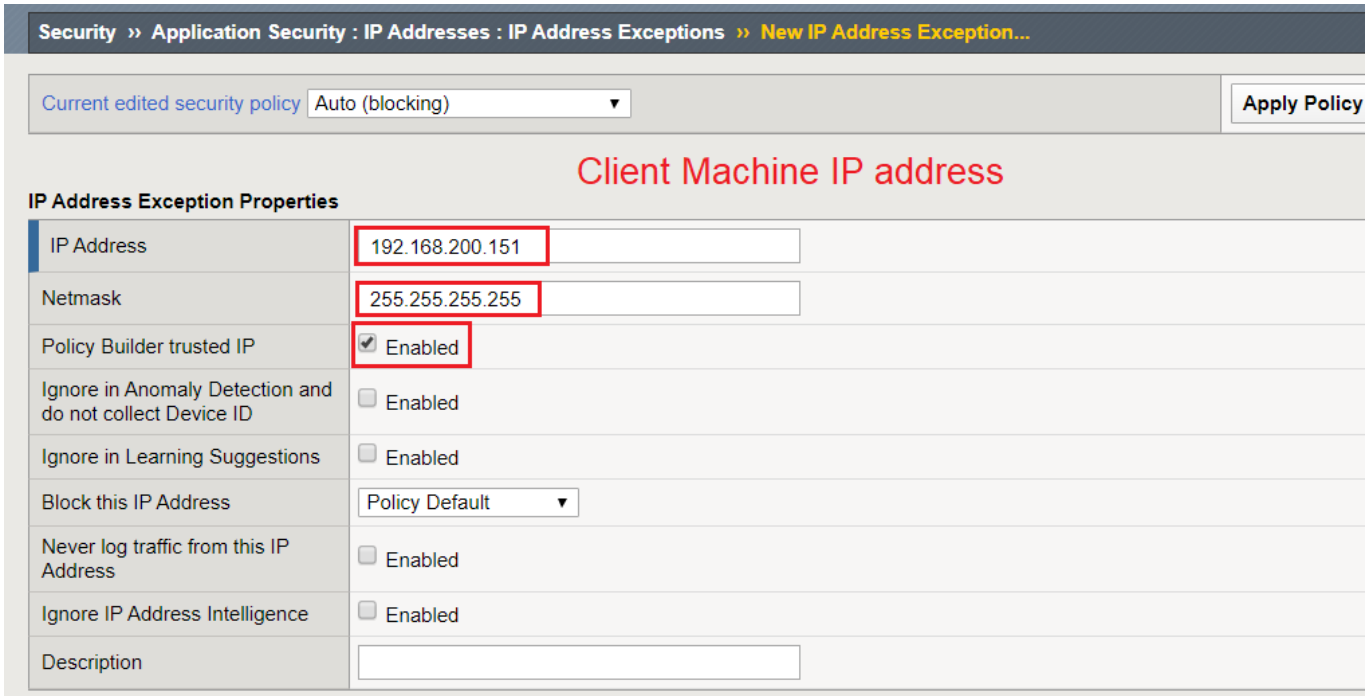
The learning score for a request from an untrusted IP Address will increment very slowly to 100 percent while ASM tracks the frequency and severity of violations. To rapidly increase the progress to 100 percent you can add a trusted IP Address.

---

7. On the **traffic learning** screen, delete all suggestions.

Add a Trusted IP Address

8. Go to **Security>>Application Security: IP addresses : IP Address Exceptions** and click **Create**
9. Specify Client IP address [Desktop/Laptop used to access auction site] with /32 subnet mask
10. Enable **Policy Builder trusted IP**



11. Click **Apply Policy**.

Send request after adding a trusted IP Address

Lab 16: TPS Based Denial of service Mitigation

Lab Objectives:

- Configure a DoS profile for TPS- based Anomaly protection
- Enable DoS profile on the virtual server
- Create a DoS logging profile
- Tune settings for TPS Anomaly detection
- Trigger a violation
- View results

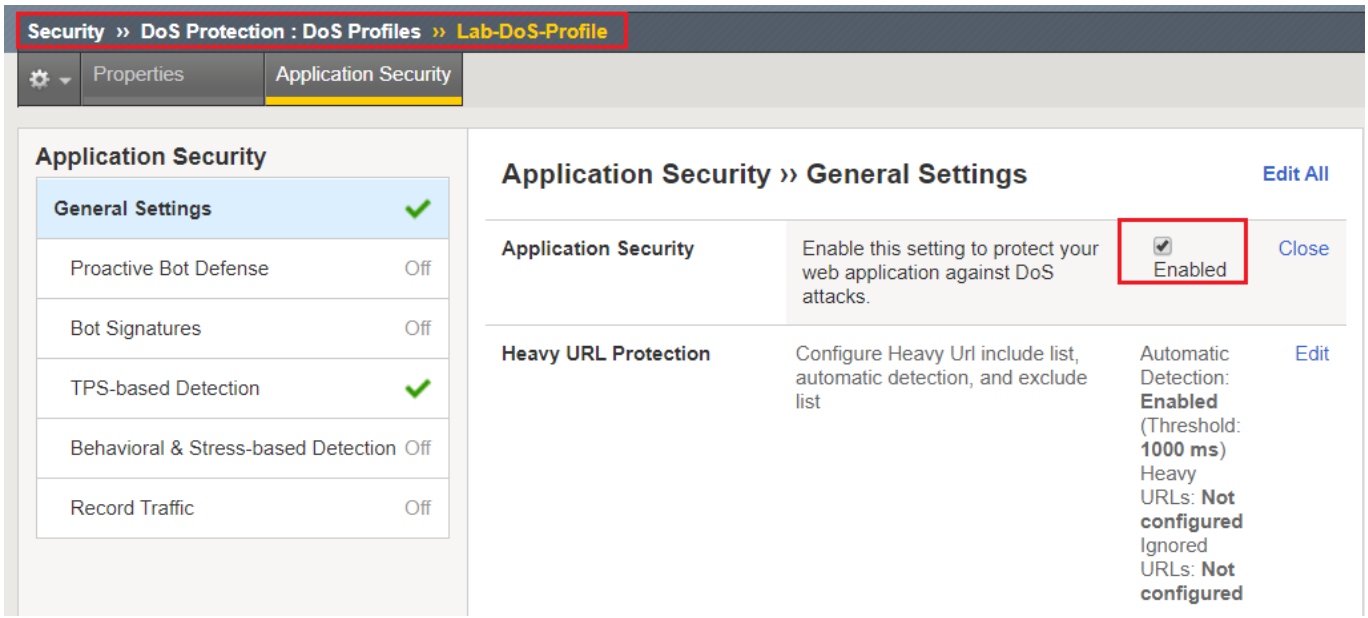
Lab Requirements:

- Access to the auction site via a working Virtual server with Application Security policy enabled.
- Access to the Firefox browser and the iMarcos add-on or HTTrack.

For all previous labs Application security policy has been enabled in order to associate specific security policies with the virtual server. However, it is important to note that L7 Dos Profile can coexist with L7 Application security policies, and L7 Application security policies are not required if you would like to only use and L7 DoS Profile.

Create a DoS Profile

1. Go to **security>>DoS Protection: DoS Profiles and then click Create**.
2. Give your profile a name.
3. On the left side of the screen, locate **Application Security**.
4. Click General Settings.
5. On the Right side of the screen, note that Application Security is disabled.
6. Click **Edit**.
7. Click the **enabled** checkbox.



Configure TPS- based Detection

8. On the left side of the screen, click TPS-based Detection.

We will now configure mitigation based on a source IP address and URL.

9. Locate the By Source IP Row and then click create.
10. Configure the following settings for **By Source IP**

    Relative Threshold TPS increased by: **5%**
    and reached at least **2** Transactions per second
    or Absolute Threshold TPS reached **2** transactions per second
    Enable **CAPTCHA Challenge**

11. Ensure that the setting for Request Blocking is **Block All**

12. Locate the By URL row and then Click Edit.
13. Configure the following settings for By URL

    Relative Threshold TPS increased by: **5%**