# CIS 480 Project – Injection 3

## Introduction

All right, team! It has been reported that the e-commerce server has a lot of vulnerabilities. It’s amazing that you have been claiming big paychecks by keeping those vulnerabilities. Let’s test how serious the vulnerabilities are.

## Tutorials

* Metasploit

1. Watch the following video to learn about Metasploit.

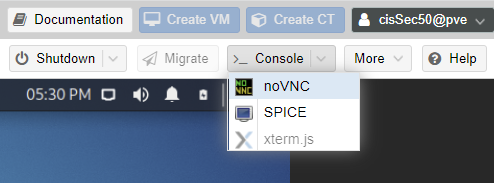
* <https://www.youtube.com/watch?v=TieUDcbk-bg&ab_channel=LoiLiangYang>

1. Watch the following video for initial 20-30 minutes for an overview of the tool. You may skip if you are familiar with it.

* <http://www.irongeek.com/i.php?page=videos%2Fintro-to-metasploit-class-at-iu-southeast>
* Bind vs reverse shell.

<https://irichmore.wordpress.com/2015/06/04/bind-shell-vs-reverse-shell/>

* The screen can be detached by selecting **noVNC**.



## Additional

* Each team needs to designate an account for the team and use it to address the injections. Everyone in the team can login to the account using the same credentials and work together.
* Everyone needs to participate. At the end, peer evaluation will be requested.
* To switch into a superuser, type **sudo su**, followed by **kali/kali** for the credentials.

## Injection

1. Start Kali and e-commerce server.
2. Please break into the server, not by a hammer but by a keyboard. To break into the server, use Metasploit on Kali. You are not supposed to log in to the e-commerce server.

## Steps/Hints

1. Use the steps below to use Metasploit.
2. You need to start the databases service to store all the results. Use this command: **systemctl start postgresql**.
3. To run Metasploit for the first time, you need to create a database schema. Use this command: **msfdb init**.
4. You start the Metasploit by running this command: **msfconsole**.
5. You can exploit any vulnerabilities that are present on the server. First, you need to research vulnerabilities for the services on the server and then, collect guidance about how to exploit them. There are plenty of websites and YouTube videos that explain how to break into the server taking advantage of the vulnerabilities using Metasploit.
6. There are multiple ways to break into the server.
   1. One way is to use the files in the following directory: **/home/kali/Documents**. The text files **passdic-wk1.txt** and **userid.txt** are relevant to this injection.
   2. Use **stop\_on\_success** option before running **exploit** as necessary: **set stop\_on\_success true.**
7. After getting the (reverse) shell from the server, try the following commands to check the account that is associated with the intrusion on the server.

* Commands to test: whoami, id, pwd, and ls.

1. Show the reverse shell in a screenshot.
2. Execute the commends: whoami, id, pwd, and ls.
3. Follow the naming convention for the submission of. Use this format: CIS480Prj-classX-injY-teamZ.docx, where X is 1 for sec01 and 2 for sec76, Y is injection number, and Z is your team number on the team roster.)
4. *Leave the current terminals on Kali as they are for Injection 4. Injection 4 is based on current intrusion.*

## Response to Injection 3

1. Team members: *list names here.*

Jon McCarrick

Jacob Ornstein

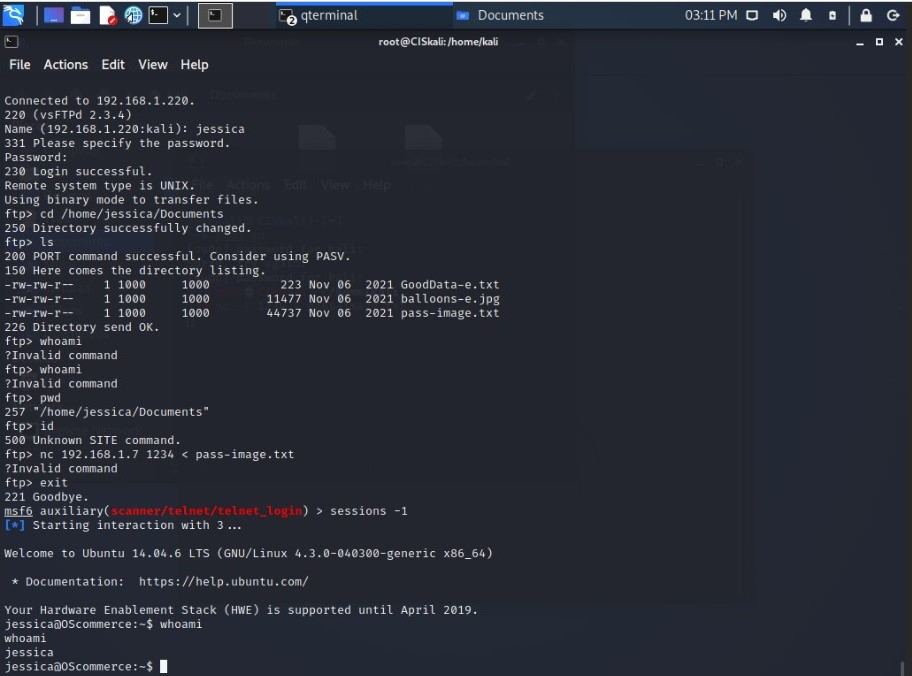
Stephen Welsh

1. Show the reverse shell in a screenshot.



The shell is in the screenshot below

1. Execute the commends (whoami, id, pwd, and ls) and report the output on a screenshot.



## Logistics

|  |  |  |
| --- | --- | --- |
| **Injections** | **Post** | **Due (midnight)** |
| Injection 1 – Introduce the team | Mon, 7th | Tue, 8th |
| Injection 2 – Scan the network | Tue, 8th | Wed, 9th |
| Injection 3 – Break into the target | Wed, 9th | Fri, 11th |
| Injection 4 – File transfer | Wed, 9th | Fri, 11th |
| Injection 5 – Treasure hunt | Thur, 10th | Sat, 12th |