

# Penetration Testing Lab

## Reconnaissance and Mapping

### Using Samurai-2.0

#### Notes:

1. Be careful about running most of these tools against machines without permission. Even the poorest intrusion detection system will report some of these tests.
2. Login and password for the live CD is samurai and samurai.
3. For every command, there should be a man page. Look it over to see the syntax and options for the command.
4. The target assumed is DVWA wherever you have it.
  - a. The target will be called "dvwa.yourdomain.xxx"
  - b. One option is to install it on your machine and then install Samurai in a container like vmware or Virtual Box or Parallels.
  - c. Another option is to open the Samurai iso file, but DVWA in the root and configure the web server and then recreate the iso with DVWA neatly included. I haven't done this yet, so try at your own risk.
  - d. In this first lab, many of the commands could be run against a local machine without it having to have DVWA.
5. If you use windows, you may want to install Cygwin to get Linux tools
  - a. <http://www.cygwin.com/> has instructions
6. Goals:
  - a. Get a handle on reconnaissance and mapping
  - b. Learn to use a few tools
  - c. Have some fun (no, really)

## Reconnaissance

### **Exercise 1: nslookup**

1. Enter the command:  
    `nslookup dvwa.yourdomain.xxx`
  - a. What is the IP address of our default DNS server? What does that mean?
  
  
  
  
  
  
  
  
  
  
  - b. What is the IP address of `dvwa.yourdomain.xxx`?
  
2. Enter nslookup interactive mode by entering:  
    `nslookup`  
and then:  
    `set debug`  
Now enter the following request:  
    `dvwa.yourdomain.xxx`
  - a. How many authoritative nameservers are there for the `cs.montana.edu` domain?
  
  
  
  
  
  
  
  
  
  
  - b. Their names and IP addresses?
  
  
  
  
  
  
  
  
  
  
- c. Enter `montana.edu` and answer the same questions.

## **Exercise 2: dig**

1. Run `man dig` to see the syntax of the command.
  
2. Enter `dig dwwa.yourdomain.xxx` and compare the output to `nslookup`.
  
3. Enter `dig montana.edu mx`.
  - a. What are the DNS names and IP addresses of the campus mail servers?
  
4. Enter `dig cs.montana.edu ANY +answer`.
  - a. What did you find out?



## Exercise 4: netcat

1. Open a terminal if you need one.

Enter `nc google.com 80`

Enter :

```
HEAD / HTTP/1.0
```

and hit enter twice.

- a. What do you see?

netcat allows you to build an HTTP request manually from stdin. You need a blank line to trigger the send. Try the following:

```
nc google.com 80
```

```
GET / HTTP/1.1
```

```
Host: google.com
```

```
User-Agent: BOZOS-BROWSER
```

```
Referrer: MasterOfDisguise.com
```

- b. <http://www.google.com/#hl=en&source=hp&q=netcat>



# Mapping

## Exercise 1: wget

1. wget downloads files via HTTP, HTTPS or FTP. Check out the man page. Create a directory to store downloaded data in.
2. Enter  
wget <http://www.dvwa.yourdomain.xxx/~harkin/assignment1/insert.html>
3. Now try the recursive option:  
wget -r <http://www.dvwa.yourdomain.xxx/~harkin/assignment1/> --no-check-certificate
  - a. Look to see what is stored? How cool is that? What is in the various delete.php files? What has happened here?

## **Exercise 2: webscarab**

Return to the home directory and enter the following:

```
java -jar /usr/bin/samurai/webscarab/webscarab-(hit the Tab key here)
```

Now launch Firefox. Go to Tools > SwitchProxy > WebScarab Local