



PRIFYSGOL CYMRU
Y Drindod Dewi Sant
UNIVERSITY OF WALES
Trinity Saint David
SWANSEA - ABERTAWE

Applied Computing

Wales Institute of Science and Art (WISA)

Advanced Cybersecurity (ACCB6000)

Lab 8: Into the Web



Nitheesh Murugan Kaliyamurthy – n.kaliyamurthy@uwtsd.ac.uk

Cisco | **Networking Academy**[®]
Mind Wide Open[™]



What we do?

1. *Set up*
2. *Webserver Reconnaissance*
3. *Webserver Hacking*

Disclaimer

Do not try these in unsupervised environments/ real time environments. Attempting to use certain tools in real time environments or without proper written consents from the owners of the network is punishable offense. All our labs are only for educational purposes and to be practiced under supervised environments.

Takeaway



Maintenance (Manual) is now available to all students of this class to refer, add your experience and share your reflections. DON'T FORGET TO ADD YOUR NAME IN YOUR POST. Each poster will be awarded with for their work.

Link is shared in our Teams Channel!!!

Recommendations

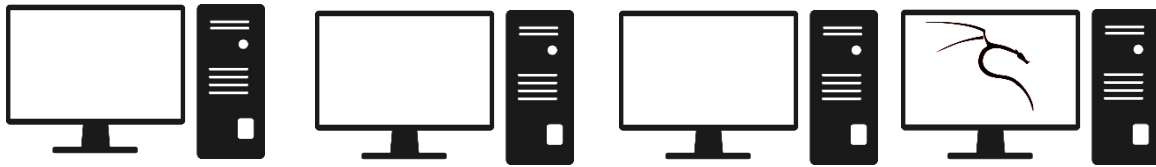
You could use any of the following as per your convenience. Highlighted is used here.

- ✓ **VirtualBox**
- ✓ VMware Workstation Pro
- ✓ VMware Fusion Pro (for Mac),
- ✓ VMware ESXi
- ✓ Microsoft Hyper-V

What you need?

- Virtual Machines running Kali Linux (*Attacker*), Windows Server 2012, Windows Server 2016, Ubuntu, Windows 10, Windows 8, Windows 7 (Optional), Windows XP (Optional).
- Internet access

The configurations/ ip addressing below listed is based on this topology. Make necessary changes as you work on.



<u>Win 7 (Opt)</u>	<u>Win Sr 2012</u>	<u>Win Sr 2016</u>	<u>Win 10</u>
<u>10.0.2.7</u>	<u>10.0.2.10</u>	<u>10.0.2.9</u>	<u>10.0.2.8</u>
<u>10.0.2.1</u>	<u>10.0.2.1</u>	<u>10.0.2.1</u>	<u>10.0.2.1</u>

<u>Kali</u>	<u>Ubuntu</u>	<u>XP (Opt)</u>	<u>Win 8</u>
<u>10.0.2.15</u>	<u>10.0.2.14</u>	<u>10.0.2.6</u>	<u>10.0.2.11</u>
<u>10.0.2.1</u>	<u>10.0.2.1</u>	<u>10.0.2.1</u>	<u>10.0.2.1</u>

- **Network Settings: Nat Network; allow all VM's**
- **Follow the instructions step – by – step. If you miss one step, you will not be successful in completing this lab.**
- **Recommendations: Use the latest tools/ softwares (if available)**
- **If any errors, troubleshoot and record it.**
- *Hint: You could do this document as a part of your coursework. Need not submit this in Moodle. While building and configuring the lab setup, document it and use it in your course work.*

Contents

Virtual Box (Latest Version)	5
OS:	5
Network Settings:	7
Other Settings:	7
Users	7
Password Complexity	7
Windows Explorer	8
Active Directory	8
Install Active Directory	8
Group Policy Mgt	9
AD User accounts	9
SNMP	9
SQL Server	9
Turn off Firewalls	10
Enable Remote Desktop Connection	11
Enable FTP Server	11
Install Supporting Tools	12
Linux Editor	12
Acrobat Reader	12
Winrar	12
Web Browsers	12
Websites for Demo	12
Goodshopping Website	12
Moviescope Website	13
Host Files	14
Windows Server 2016, 2012	14
Windows 10, 7, XP (Optional)	14
Kali Linux	14
Ubuntu Linux	15
WAMP Server	15
Windows Server 2012	15
Wordpress	15
Databases	15
Go to c:\wamp64\www	16
Go to browser: http://localhost:8080/wordpress	16

Give the db details	16
Give the site details.....	16
Create users with different roles	17
Damn Vulnerable Web Application	17
Databases.....	17
Go to c:\wamp64\www	17
Go to c:\wamp64\www\dvwa\config.....	17
Go to browser: http://localhost:8080/dvwa/setup.php	18
Go to browser: http://localhost:8080/dvwa/login.php.....	18
Final Setup.....	18
Turn off (All Windows).....	18
Test.....	18

Virtual Box (Latest Version)

OS:

Windows Server 2016	10.0.2.9	255.255.255.0	10.0.2.1
Windows Server 2012	10.0.2.10	255.255.255.0	10.0.2.1
Windows 10	10.0.2.8	255.255.255.0	10.0.2.1
Windows 8.1	10.0.2.11	255.255.255.0	10.0.2.1
Windows 7 (Optional)	10.0.2.7	255.255.255.0	10.0.2.1
Windows XP (Optional – to check the legacy settings)			

Kali Linux **10.0.2.15** **255.255.255.0** **10.0.2.1**

```
password  
(kali, root, toor, password)  
Goto Terminal → etc/network/  
sudo vim interfaces  
auto eth0  
allow-hotplug eth0  
iface eth0 inet static  
address 10.0.2.14  
netmask 255.255.255.0  
gateway 10.0.2.1  
nameserver 8.8.8.8
```

Ubuntu Linux **10.0.2.14** **255.255.255.0** **10.0.2.1**

```
password  
sudo gedit /etc/network/interfaces  
auto ens33  
allow-hotplug ens33  
iface ens33 inet static  
address 10.0.2.14  
netmask 255.255.255.0  
gateway 10.0.2.1  
dns-nameservers 8.8.8.8 8.8.4.4
```

Network Settings:

Configure Nat

Shared Folders (Different ways to share folder. Refer to a video describing few methods)

Optional: Add your method in the Onenote

Other Settings:

Change Computer Names and assign to Workgroup

Servers: (Eg: For Server 2016 WinSer)

Users (Create test users)

Windows Server 2016

Windows 10, 7

Control Panel → User Accounts → Create Local Accounts

Password Complexity

Windows Server 2016, 2012

Windows 10, 7

Windows Administrative Tools → Local Security Policy → Account Policy

→ Password Policy:

Password must meet complexity req. (Disable)

Max Password Age

Min Password Age

Windows Explorer

Windows Server 2016, 2012

Windows 10, 7, XP (Optional)

Control Panel → File Explorer Option → Advanced Settings

Check/Enable

Show Hidden Files/ Folders

Hide Empty Drives

Hide folder merge conflicts

Show drive letters

Show pop-up desc

uncheck/Disable

Hide Extensions

Hide protected os files

Active Directory

Windows Server 2012

Install Active Directory

Server Manager → Add roles and features

Role based or feature based

Select the server from the pool (Select your server)

Active Directory Domain Services

.Net 3.5, 4.5

Group Policy Mgt

Restart the dest. Server

Install

Post Deployment Configurations

Promote this server to a domain controller

Select your server and type the password

NetBIOS Name: ACCB6000

Install

Restart and Login to check ACCB6000\Admin

Group Policy Mgt

Administrative Tools→Group Policy Mgt→ Forest:ACCB6000.com

Default Domain

Settings → Edit

Enforce Password history → 0

Max Password Age → 0

Min Password Age → 0

Password must meet complexity req. (Disable)

AD User accounts

Administrative Tools→Active Directory Users and Computers

Accb6000.com → users→new→ user

Create users and select the users property and add as Administrator in the Member of tab

SNMP

Windows Server 2012, 2016

Services → SNMP Service→ Properties→Security → Add

Community Name: Public

Community Rights: Read only

Accept SNMP Packets from any hosts

SQL Server

Windows Server 2016

Custom Installation

New Standalone

Updates: No Updates

Feature Selection: All Features Selection

DB Engine: Mixed Mode

Add Current User

Accept

Install SQL Server Mgt Tools

Download SQL Server Mgt Studio ...

Install

Open Server Mgt Studio

New Query

```
EXEC sp_configure 'show advanced options', 1
```

```
GO
```

```
RECONFIGURE
```

```
GO
```

```
EXEC sp_configure 'xp_cmdshell', 1
```

```
GO
```

```
RECONFIGURE
```

```
GO
```

Execute the Query

Turn off Firewalls

Windows Server 2012, 2016

Windows 10, 7, XP (Optional)

Enable Remote Desktop Connection

Windows Server 2012, 2016

Windows 10, 7, XP (Optional)

Enable FTP Server

Windows 10

Turn on windows features

.NET Framework 3.5, 4.6

IIS

FTP Server

Web Mgt Tools

World Wide Web

Download (If required)

Restart

Control Panel → Administrative Tools → IIS Manager

Sites → Add FTP Sites → localhost

Select Path (C: Create a new folder and name it FTP)

IP Address of the local machine

Start Automatically

No SSL

Basic

Read and Write

All Users

Install Supporting Tools

Linux Editor

apt-get install vim

Acrobat Reader

Windows Server 2016, 2012

Windows 10, 7, XP (Optional)

Winrar

Windows Server 2016, 2012

Windows 10, 7, XP (Optional)

Web Browsers

Windows Server 2016, 2012

Windows 10, 7, XP (Optional)

Firefox, Chrome

Websites for Demo

Windows Server 2016

Goodshopping Website

Setup.exe

C:\inetpub\wwwroot\GoodShopping → Web.config

Open with notepad

ConnectionString: Set, Data Source as your host machine name, password and user id as configured in your SQL

Save

Open default.aspx.cs in notepad

In the public protected (I24) replace localhost with your Server 2016 ip address

Open SQL Server Mgt Studio

New Database

GoodShopping

Options: Simple

Create Database and Restore the goodshopping.bak file

Make sure in the options, allow to overwrite the existing database

IIS Manager

Add Website from the machine name

Site Name: GoodShopping

Select the folder from C:\inetpub\wwwroot

http protocol; host ip address; port 80

hostname as www.goodshopping.com

Start website immediately

Moviescope Website

Setup.exe

C:\inetpub\wwwroot\moviescope → Web.config

Open with notepad

ConnectionString: Set, Data Source as your host machine name, password and user id as configured in your SQL

Save

Open SQL Server Mgt Studio

New Database

moviescope

Options: Simple

Create Database and Restore the moviescope.bak file

Make sure in the options, allow to overwrite the existing database

IIS Manager

Add Website from the machine name

Site Name: moviescope

Select the folder from C:\inetpub\wwwroot

http protocol; host ip address; port 80

hostname as www.moviescope.com

Start website immediately

Host Files

Windows Server 2016, 2012

C:\Windows\System32\drivers\etc→ hosts

Open with notepad

Add at the end

IP Addressof the Win Ser 16 www.goodshopping.com

IP Addressof the Win Ser 16 www.moviescope.com

127.0.0.1 fonts.googleapis.com

Windows 10, 7, XP (Optional)

C:\Windows\System32\drivers\etc→ hosts

Copy the file and paste it in desktop

Open with notepad

Add at the end

IP Addressof the Win Ser 16 www.goodshopping.com

IP Addressof the Win Ser 16 www.moviescope.com

127.0.0.1 fonts.googleapis.com

Paste it back in its folder

Kali Linux

Etc → Hosts

Add at the end

IP Addressof the Win Ser 16 www.goodshopping.com

IP Addressof the Win Ser 16 www.moviescope.com

127.0.0.1 fonts.googleapis.com

Ubuntu Linux

Sudo gedit /etc/hosts

Add at the end

IP Address of the Win Ser 16 www.goodshopping.com

IP Address of the Win Ser 16 www.moviescope.com

127.0.0.1 fonts.googleapis.com

WAMP Server

Windows Server 2012

Download and install Wamp Server

Wamp Server → Tools → Ports used by apache → Desired Port Number 8080

C:\wamp64\bin\apache2.4....\conf → httpd.conf

Open with notepad

(Line 292 – Might vary) Required Local → Change it to Require all granted

Save and restart all the services

Wordpress

Windows Server 2012

Wamp Server → localhost

Tools → phpmyadmin → login as root; no password; enter

Login

Databases

Create Database

wordpress → collation → Create

Click on the Privileges in the created db

Add user account

Admin; select hostname as local; set password

Select Global Privileges

Go

Go to c:\wamp64\www

Create a Folder (wordpress)

Copy the wordpress file and paste it in

Go to browser: <http://localhost:8080/wordpress>

Setup Configuration page opens

DB Name: wordpress

Username: admin

Password: your password created earlier

Db host: localhost

Prefix: wp_

Run

Install

Site Name: wordpress demo

Username: admin

Password: your password created earlier

email: your email (recommend to create one)

Install

After installation: Login with your admin credentials

Go to Settings → General

Wordpress Address: <http://ip> address of your winserver
12:8080/wordpress

Site Address: <http://ip> address of your winserver
12:8080/wordpress

Login again and check if the url is updated with your ip
address.

Create users in the dashboard with roles as editor, contributor and so on.

Damn Vulnerable Web Application

Windows Server 2012

Wamp Server → localhost

Tools → phpmyadmin → login as root; no password; enter

Login

Databases

Create Database

dvwa → collation → Create

Click on the Privileges in the created db

Add user account

Dvwa_user; select hostname as local; set password

Select Global Privileges

Go

Go to c:\wamp64\www

Create a Folder (dvwa)

Copy the dvwa file and paste it in

Go to c:\wamp64\www\dw\config

Open config.inc.php.dist with notepad

Change:

Db server (L19) to localhost

Db name to dvwa

Db username to dvwa_user

Db password to your password created

Save as config.inc.php

Go to browser: <http://localhost:8080/dvwa/setup.php>

Create/ Reset Database

Go to browser: <http://localhost:8080/dvwa/login.php>

Login using your login credentials created

DVWA Security → Low

Logout

Final Setup

Turn off (All Windows)

Automatic Updates

Windows Defender

Real Time Protection

Behavior Monitoring

Scan all the downloaded files and attachments

Server Manager (Servers)

Test

Ping all the machines in your setup and it should be successful.

All the webserver/ webpages are loading as anticipated.

Active Directory is setup.

Other settings are effective.