# Ethical Hacking Lab

# Setup Guide

The purpose of this guide is to give you steps on creating your own lab environment that you can "hack" to your heart's content. Use the checkboxes to track your progress (there's a lot to do!). These are "high-level" configuration steps that should be familiar to IT Professionals

Please note: In future courses, you'll have access to an "EH-ToolsMod-X.iso". If you mount this .iso on your host machine, you might get several warnings and "issues" as most of the programs on the .iso are recognized as "spyware", "malware", and "security related" issues. Please only mount this .iso on your virtual machines....You've been warned!

#### Files needed:

- 1. Host: 1.1. http://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2012-r2
- 2. Server 2012R2 (Same as host)
- 3. Server 2008R2:
  - 3.1. http://www.microsoft.com/en-us/download/details.aspx?id=11093
- 4. Windows 8.1: 4.1. <u>http://www.microsoft.com/en-us/evalcenter/evaluate-windows-8-1-enterprise</u>
- 5. Windows 7:
  - 5.1. http://tinyurl.com/ethicalW7P1
  - 5.2. http://tinyurl.com/ethicalW7P2
  - 5.3. http://tinyurl.com/ethicalW7P3
  - 5.4. http://tinyurl.com/ethicalW7P4
  - 5.5. http://tinyurl.com/ethicalW7P5
  - 5.6. http://tinyurl.com/ethicalW7P6
  - 5.7. <u>http://tinyurl.com/ethicalW7P7</u>
- 6. Kali:
  - 6.1. https://www.kali.org/downloads

# 1) Host Machine (IP: Production IP)

Install an OS and/or application that supports Virtualization,

- Windows Server 2012 (Standard)
- o VMWare
- o Virtualbox
- If using Server 2012R2:
  - Install Standard with GUI

- Use the password of Pa\$\$w0rd
- Change the Computer Name
- Change the Time Zone
- Disable the IE ESC
- Disable Data Execution Prevention
- o Disable Complexity Requirements for passwords
- o Reboot
- Install the Hyper-V Role
  - Choose the Ethernet adapter
  - No migration options
  - Choose your VM file locations
  - Two restarts take place after you finish the wizard
- o Open Hyper-V Manager
  - Create Virtual Switch: Private Hacking Network

Rearm your trial period

- Command Prompt as Administrator
- o SImgr-rearm

# 2) Server 2012R2 (192.168.0.10/24 - DNS: 192.168.0.10)

Create a new Virtual Machine

- Select a storage location (mine was c:\ceh project\vm's)
- Use Gen1 machines
- Use 4096MB of RAM
- Use the Hacking Network
- Location of VHDX (see storage location)
  - Use defaults for Size
- o Install from .iso (Server 2012R2)

Connect and start VM

Install Server 2012R2 using Standard Server with GUI Installation

Use password of Pa\$\$w0rd for the Administrator's Account

Change the computer name to Server2012R2

Disable the IE ESC

Disable the Data Execution Prevention

Restart

Install the role of Web Server (IIS)

- o If you get an error about "alternate source path do the following:
  - Open a command prompt at administrator (assuming your source .iso is mounted as the "d" drive)
  - Type dism /online /enable-feature /featurename:NetFX3 /all /Source:d:\sources\sxs /LimitAccess

- Go down to "Specify an alternate source path" and enter "d:\sources\sxs" as the path.
- See Img2.png

Select additional features of

- o BITS
- o BitLocker Network Unlock
- o Client for NFS
- Data Center Bridging
- o Direct Play
- Enhanced Storage
- Failover Clustering
- Group Policy Management
- Ink and Handwriting Services
- Internet Printing

Install SNMP Service

- Go to Services
- Properties for SNMP
- o Add a Community Name of Public with Read Only
- Accept SNMP Packets from any Host

Set the IP Address: 192.168.0.10 / 255.255.255.0 / DNS: 192.168.0.10

#### Add the Telnet Client Feature

Disable Complexity Requirements for passwords

Create User Accounts (at least 4). These accounts are created on all VM's.

User name | Password

- o Bwayne batman
- o Dgrayson robin
- o Hjordon green
- o Ckent super

Disable the Windows Firewall

Set your time zone

Rearm your trial period

- Command Prompt as Administrator
- o SImgr –rearm

# 3) Server 2008R2 (192.168.0.15/24 - DNS: 192.168.0.1)

Create a new Virtual Machine

- Select a storage location (mine was c:\ceh project\vm's)
- Use Gen1 machines
- Use 2096MB of RAM

- Use the Hacking Network
- Location of VHDX (see storage location)
  - Use defaults for Size
- o Install from .iso (Server 2008R2)

Connect and start VM

Install Server 2008R2 using Standard Server Full Installation

Use a password of Pa\$\$w0rd for the Administrator's Account.

Change the computer name to Server2008R2

Set your time zone

Turn off IE ESC

Install SNMP Service

- Go to Services
- Properties for SNMP
- Add a Community Name of Public with Read Only
- Accept SNMP Packets from any Host

Set the IP Address: 192.168.0.15 / 255.255.255.0 / DNS: 192.168.0.10

Disable Complexity Requirements for passwords

Create User Accounts (at least 4). These accounts are created on all VM's.

- User name | Password
- o Bwayne batman
- o Dgrayson robin
- o Hjordon green
- o Ckent super

Disable the Windows Firewall

Rearm your trial period

- Command Prompt as Administrator
- o SImgr –rearm

# 4) Windows 8.1 (192.168.0.20/24 - DNS: 192.168.0.1)

Create a new Virtual Machine

- Select a storage location (mine was c:\ceh project\vm's)
- Use Gen1 machines
- Use 2048MB of RAM
- Use the Hacking Network
- Location of VHDX (see storage location)
  - Use defaults for Size

• Install from .iso (Windows 8.1)

Connect and start VM

Install Windows 8.1

Use a password of Pa\$\$w0rd for the Administrator's Account.

Change the computer name to Windows81 Set your time zone Set the IP Address: 192.168.0.20 / 255.255.255.0 / DNS: 192.168.0.10 Disable Complexity Requirements for passwords Create User Accounts (at least 4). These accounts are created on all VM's.

- User name | Password
- o Bwayne batman
- o Dgrayson robin
- o Hjordon green
- o Ckent super

Disable the Windows Firewall

# 5) Windows 7 (192.168.0.25/24 - DNS: 192.168.0.1)

Create a new Virtual Machine

- Select a storage location (mine was c:\ceh project\vm's)
- Use Gen1 machines
- Use 2048MB of RAM
- Use the Hacking Network
- Use Existing virtual hard drive
  - Select the Windows7.vhd

Connect and start VM

Logon on Admin

Password is Password1

Remove Virtual PC Integration Component.

Reboot

Change the password to Pa\$\$w0rd for the Admin Account.

Change the computer name to Windows7

Set your time zone

Set the IP Address: 192.168.0.25 / 255.255.255.0 / DNS: 192.168.0.10

Disable Complexity Requirements for passwords

Create User Accounts (at least 4). These accounts are created on all VM's.

- User name | Password
- o Bwayne batman
- o Dgrayson robin
- o Hjordon green
- o Ckent super

Disable the Windows Firewall Disable error in the Action Center Rearm your trial period

- o Command Prompt as Administrator
- o SImgr-rearm

### 6) Kali (192.168.0.50/24 - DNS: 192.168.0.1)

Create a new Virtual Machine

- Select a storage location (mine was c:\ceh project\vm's)
- Use Gen1 machines
- Use 4096MB of RAM
- Use the Hacking Network

Install from .iso (Kali)
Connect and start VM
On the Boot Menu select Graphical Install
Set the IP Address: 192.168.0.50 / 255.255.255.0 / DNS: 192.168.0.10
Set the ROOT password to Pa\$\$w0rd
Set the computer name to Kali
Set the Time Zone
Partition disk = use entire disk
All files in one partition
GRUB Boot loader = Yes
Set the computer name to Kali
Logon on as root / pa\$\$w0rd

<u>الم</u>	Add Roles and Features Wizard	_ <b>_</b> X
Select role services Before You Begin Installation Type Server Selection Server Roles Features Web Server Role (IIS) Role Services Confirmation Results	Select the role services to install for Web Server (IIS) Role services	Description CGI defines how a Web server passes information to an external program. Typical uses might include using a Web form to collect information to a CGI script to be emailed somewhere else. Because CGI is a standard, CGI scripts can be written using a variety of programming languages. The downside to using CGI is the performance overhead.
	< Previous Ne	ext > Install Cancel

Do you need to specify a	n alternate source nath? One or more installation selections are missing source	files on the destination
Before You Begin Installation Type Server Selection	To install the following roles, role services, or features on selected server, o Restart the destination server automatically if required Optional features (such as administration tools) might be displayed on this been selected automatically. If you do not want to install these optional fe	click Install. s page because they have atures, click Previous to cle
Features Web Server Role (IIS) Role Services Confirmation Results	INET Framework 3.5 Features INET Framework 3.5 (includes INET 2.0 and 3.0) INET Framework 4.5 Features ASPINET 4.5 Web Server (IIS) Management Tools IIS Management Console Web Server Application Development	