

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. <http://www.microsoft.com/en-us/evalcenter/evaluate-windows-8-1-enterprise>
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. <http://tinyurl.com/ethicalW7P7>
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)
 - VMWare
 - 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
- Disable Complexity Requirements for passwords
- 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
- Open Hyper-V Manager
 - Create Virtual Switch: Private – Hacking Network
- Rearm your trial period
 - Command Prompt as Administrator
 - Slmgr -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
 - 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)
 - 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 lmg2.png
- Select additional features of
 - BITS
 - BitLocker Network Unlock
 - Client for NFS
 - Data Center Bridging
 - Direct Play
 - Enhanced Storage
 - Failover Clustering
 - Group Policy Management
 - Ink and Handwriting Services
 - Internet Printing
- 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: 192.168.0.10 / 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 |
|-----------|----------|
|-----------|----------|

- | | |
|------------|--------|
| ○ Bwayne | batman |
| ○ Dgrayson | robin |
| ○ Hjordon | green |
| ○ Ckent | super |

- Disable the Windows Firewall
- Set your time zone
- Rearm your trial period
 - Command Prompt as Administrator
 - Slmgr -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
- 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
 - Bwayne batman
 - Dgrayson robin
 - Hjordon green
 - Ckent super
- ☐ Disable the Windows Firewall
- ☐ Rearm your trial period
 - Command Prompt as Administrator
 - Simgmgr -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
 - Bwayne batman
 - Dgrayson robin
 - Hjordon green
 - 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
 - Bwayne batman
 - Dgrayson robin
 - Hjordon green
 - Ckent super

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

- Command Prompt as Administrator
- Simgmgr -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



