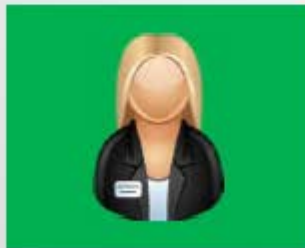


Welcome to Certified Ethical Hacker Class!

Student Introduction



Unmask the **Invisible Hacker.**



Introduction



- Name
- Company Affiliation
- Title / Function
- Job Responsibility
- System security related experience
- Expectations



Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Course **Materials**



**Identity
Card**



**Student
Courseware**



**Lab Manual/
Workbook**



**Course
Evaluation**



**Reference
Materials**

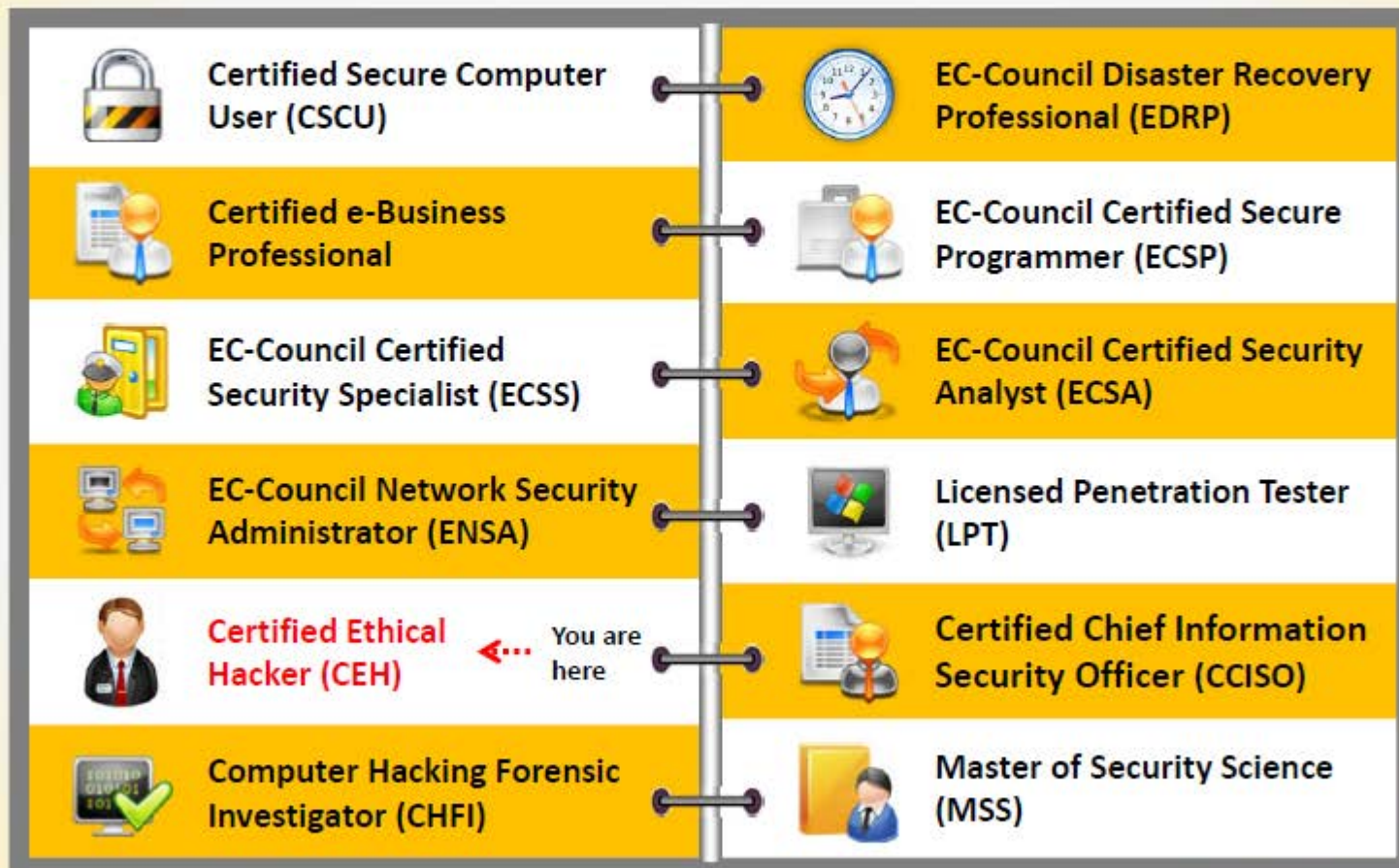
CEHv9 Course Outline

**01****Introduction to Ethical Hacking****07****Sniffing****13****SQL Injection****02****Footprinting and Reconnaissance****08****Social Engineering****14****Hacking Wireless Networks****03****Scanning Networks****09****Denial-of-Service****15****Hacking Mobile Platforms****04****Enumeration****10****Session Hijacking****16****Evading IDS, Firewalls, and Honeypots****05****System Hacking****11****Hacking Webservers****17****Cloud Computing****06****Malware Threats****12****Hacking Web Applications****18****Cryptography**

EC-Council Certification Program



There are several levels of certification tracks under the **EC-Council Accreditation** body:



Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Certified Ethical Hacker Track



CEH Certification Track

Complete the following steps:

Attend the Ethical Hacking and Countermeasures Course



Pass the CEH Exam
312-50 (ECC Exam Portal) /
312-50 (VUE)



Start

Attend
Training

Prepare for
312-50 Exam

Take
Exam

Fail

Pass

Certification
Achieved



CEHv9 Exam Information



Exam Title: **Certified Ethical Hacker**



Exam Code: **312-50 (ECC Exam Portal) / 312-50 (VUE)**



Number of Questions: **125**



Duration: **4 hours**



Availability: **ECC Exam Portal / VUE**



Passing Score: **70%**



The training center / instructor will advise you about the exam schedule and voucher details



This is a **difficult** exam and requires extensive knowledge of CEH Core Modules

Student Facilities



Class
Hours



Building
Hours



Phones



Parking



Messages



Restrooms

Smoking



Meals



Recycling



Lab Sessions



- Lab Sessions are designed to **reinforce** the classroom sessions
- The sessions are intended to give a **hands on experience** only and does not guarantee proficiency
- There are tons of labs in the lab manual. Please practice these labs back at home.



What Does **CEH** Teach You?



Network Security

Defense, Cisco Security, Firewalls, IDS, Logs, Network, Antivirus, Hardware, Troubleshooting, Availability, Server/Client Security, creating policies, network Management etc.....

Denial of Service, Trojans, Worms, Virus, Social Engineering, Password cracking, Session Hijacking, System failure, Spam, Phishing, Identity theft, Wardriving, warchalking, bluejacking Lock picking, Buffer Overflow, System hacking, Sniffing, SQL Injection.....

Ethical Hacking



This is What CEH Teaches You!

What CEH is **NOT**?



CEH class is NOT a **Network Security** training program

- Please attend EC-Council's **ENSA** class for that



CEH class is NOT a **Security Analysis** training program

- Please attend EC-Council's **ECSA** class for that



CEH class is NOT a **Security Testing** training program

- Please attend EC-Council's **LPT** Exam for that



CEH class is 100%
NETWORK OFFENSIVE
Training Program



Remember This!

**The CEH Program Teaches you 100%
Network Offensive Training and not
Defensive**

CEH Class **Speed**



The CEH class is **extremely fast paced**



The class “**speed**” can be compared to the climax scene from the movie Mission Impossible (Bullet train sequence)



There are tons of hacking **tools** and hacking **technologies** covered in the curriculum



The instructor **WILL NOT** be able to demonstrate **ALL** the tools in this class



He will showcase only **selected tools**



The students are required to **practice with the tools** not demonstrated in the class on their own

Live Hacking Website



- Please target your exercises for “Live Hacking” to www.certifiedhacker.com
- This website is meant for the students to try the tools on live target
- Please refrain from using the exploits on any other domains on the Internet



**CEH Classroom
Attack Lab
Website**

NDA Document



Please read the contents of the provided EC-Council's CEH NDA document

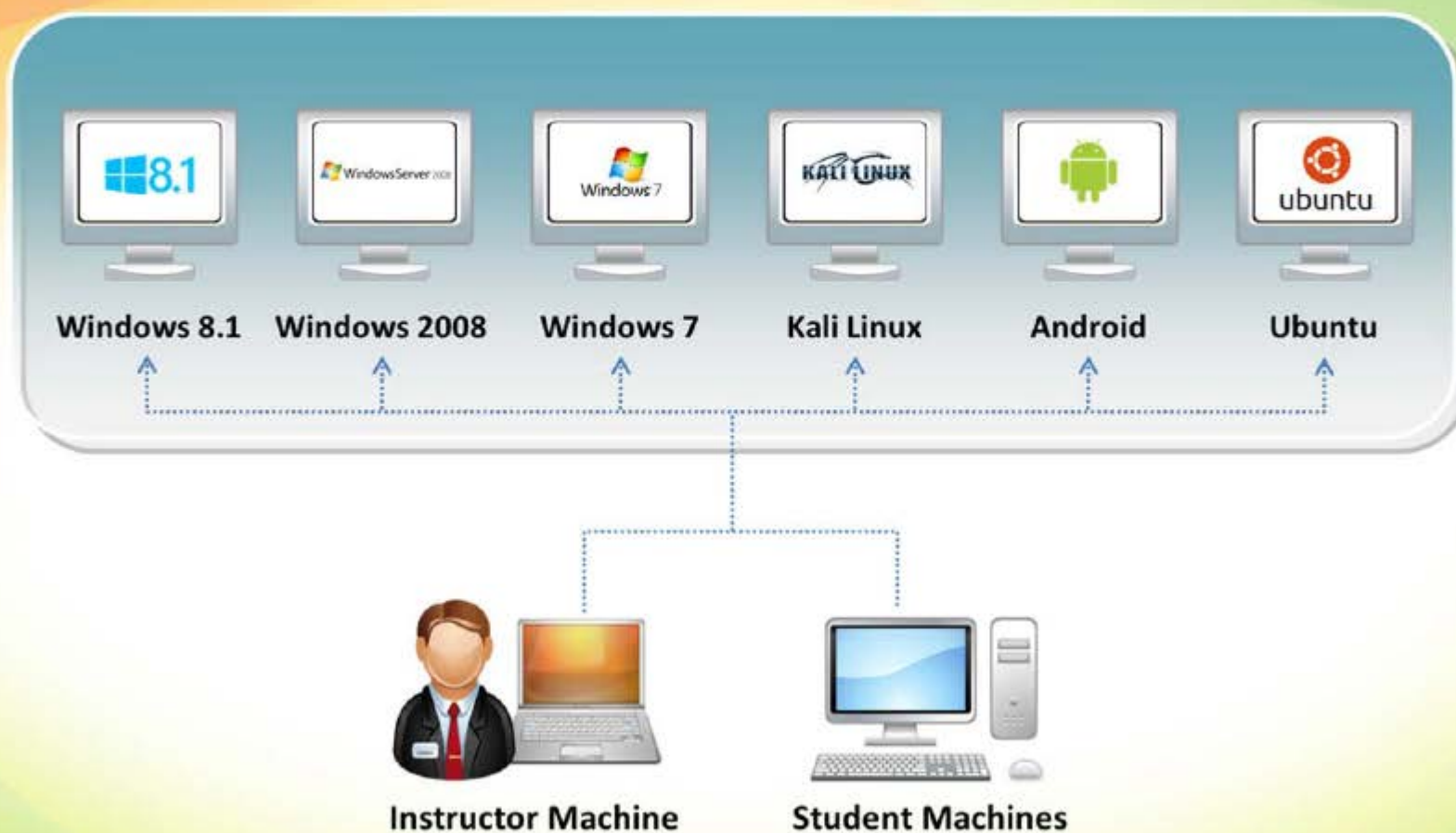
Sign this document and hand it over to the instructor

We will NOT start the class unless you sign this document

Please approach the instructor if you are not presented with this document



Advanced Lab Environment



Instructor and Student Machine Operating System: Windows Server 2012 (Fully Patched)

Student Computer Checklist



Check if your machine has the following OSeS installed (Fully Patched)



Windows Server 2012 as host

Windows Server 2008 as VM



Windows 8.1 as VM



Windows 7 as VM

Kali Linux as VM



Android as VM

Ubuntu as VM

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Student Computer Checklist

**1**

Write down IP addresses of the **host** and all the **Virtual Machines**

2

Check if you can ping between the **VM** and the **hosts**

3

Make sure that you can access **D:\CEH-Tools** directory in **Windows Server 2012** and **Z:\CEH-Tools** from all the VM's; **Z:** is mapped **Network Drive** containing **CEH tools**

4

Check if you can launch **command shell** by right clicking on a folder

5

Check if you can access **Internet** and browse the web using **IE, Chrome, Safari** and **Firefox**

6

Check for **Checkpoints** of **Virtual Machines**

7

Check if you can access <http://www.certifiedhacker.com>

8

Make sure you can access **Moviescope** and **GoodShopping** websites at <http://www.moviescope.com> and <http://www.goodshopping.com>



Ping Between Virtual Machines and Host



```
Administrator: Command Prompt
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>ping 10.0.0.10

Pinging 10.0.0.10 with 32 bytes of data:
Reply from 10.0.0.10: bytes=32 time<1ms TTL=128
Reply from 10.0.0.10: bytes=32 time<1ms TTL=128
Reply from 10.0.0.10: bytes=32 time<1ms TTL=128
Reply from 10.0.0.10: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.0.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Windows\system32>
```

```
Administrator: Command Prompt
Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ping 10.0.0.10

Pinging 10.0.0.10 with 32 bytes of data:
Reply from 10.0.0.10: bytes=32 time<1ms TTL=128
Reply from 10.0.0.10: bytes=32 time<1ms TTL=128
Reply from 10.0.0.10: bytes=32 time<1ms TTL=128
Reply from 10.0.0.10: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.0.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Administrator>
```

```
Administrator: Command Prompt
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>ping 10.0.0.9

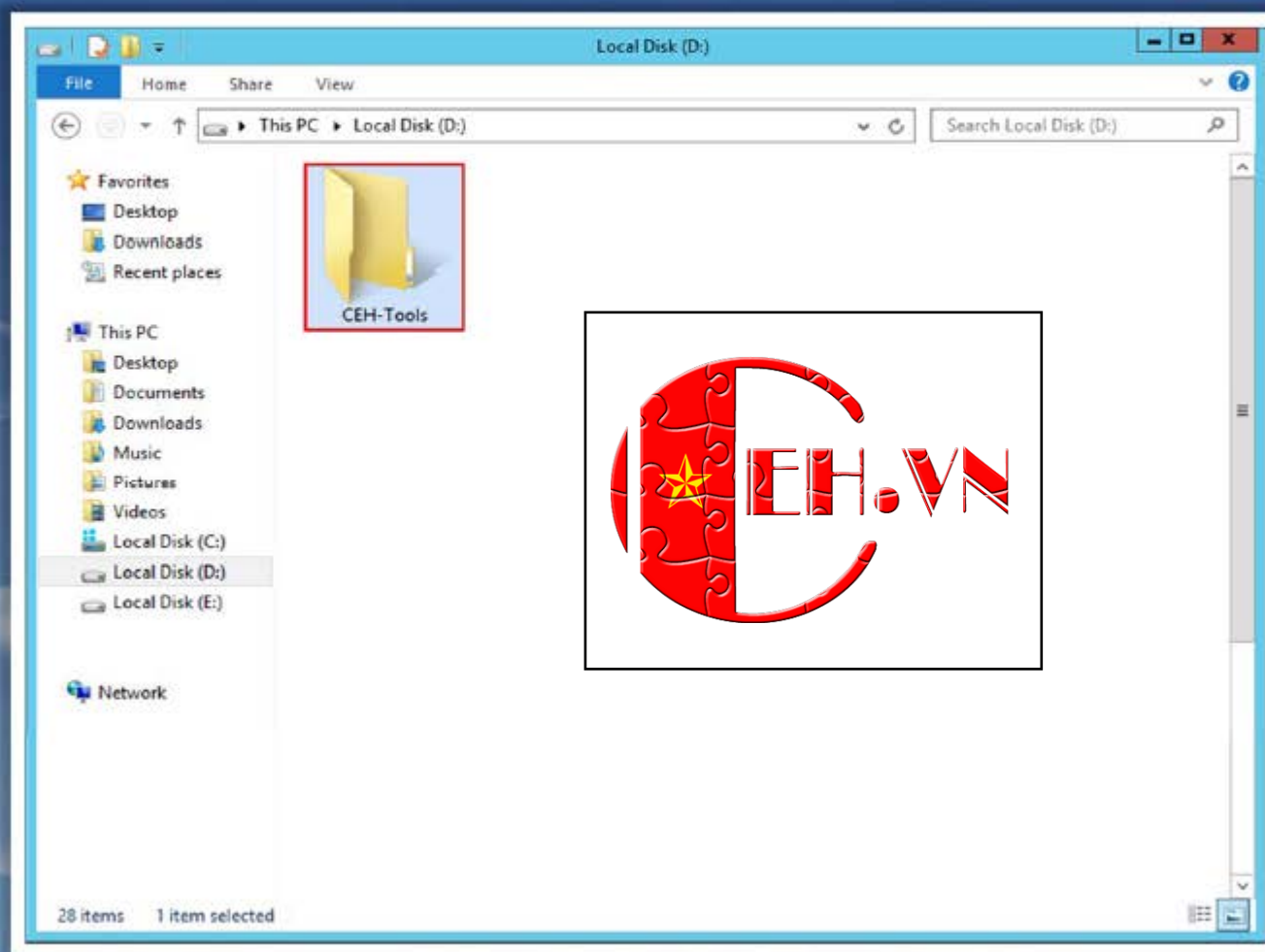
Pinging 10.0.0.9 with 32 bytes of data:
Reply from 10.0.0.9: bytes=32 time<1ms TTL=128
Reply from 10.0.0.9: bytes=32 time<1ms TTL=128
Reply from 10.0.0.9: bytes=32 time<1ms TTL=128
Reply from 10.0.0.9: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.0.9:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Windows\system32>
```

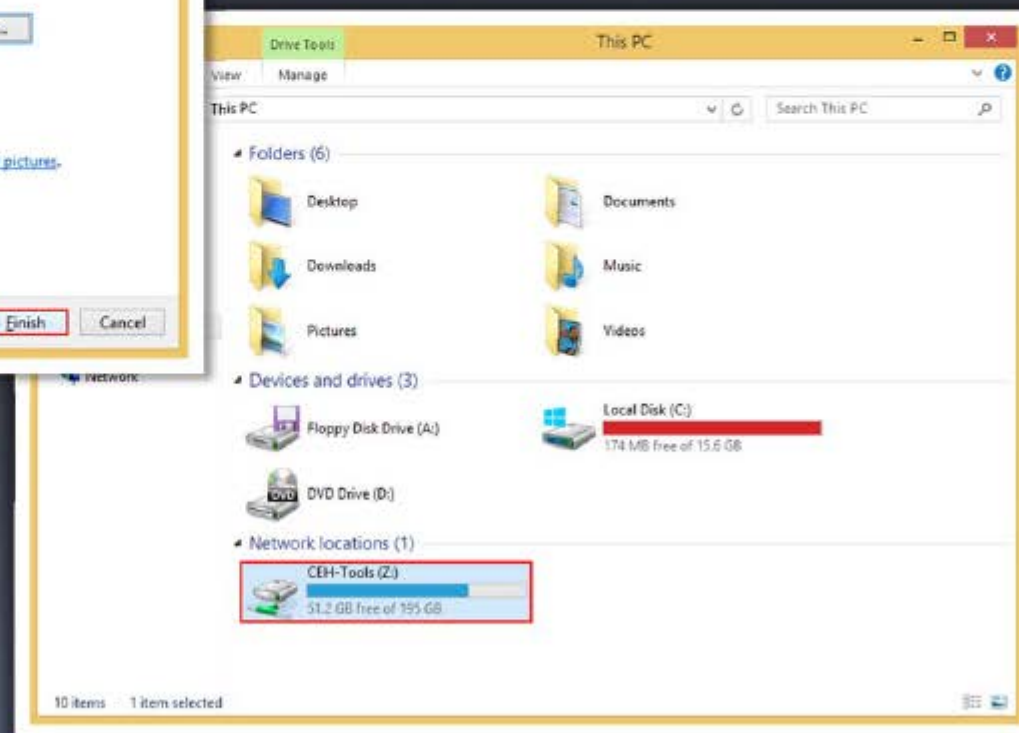
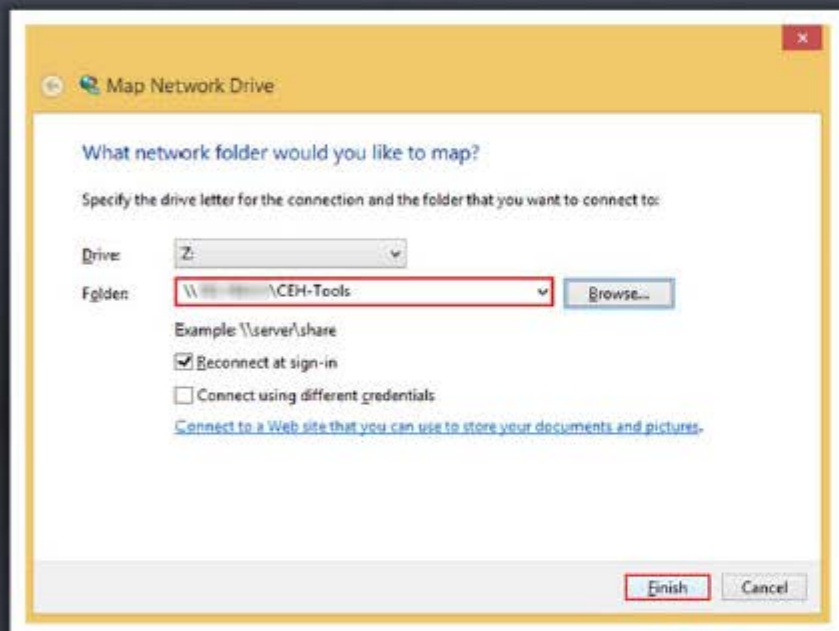
Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

CEH-Tools Directory in Windows Server 2012 (D:\CEH-Tools)



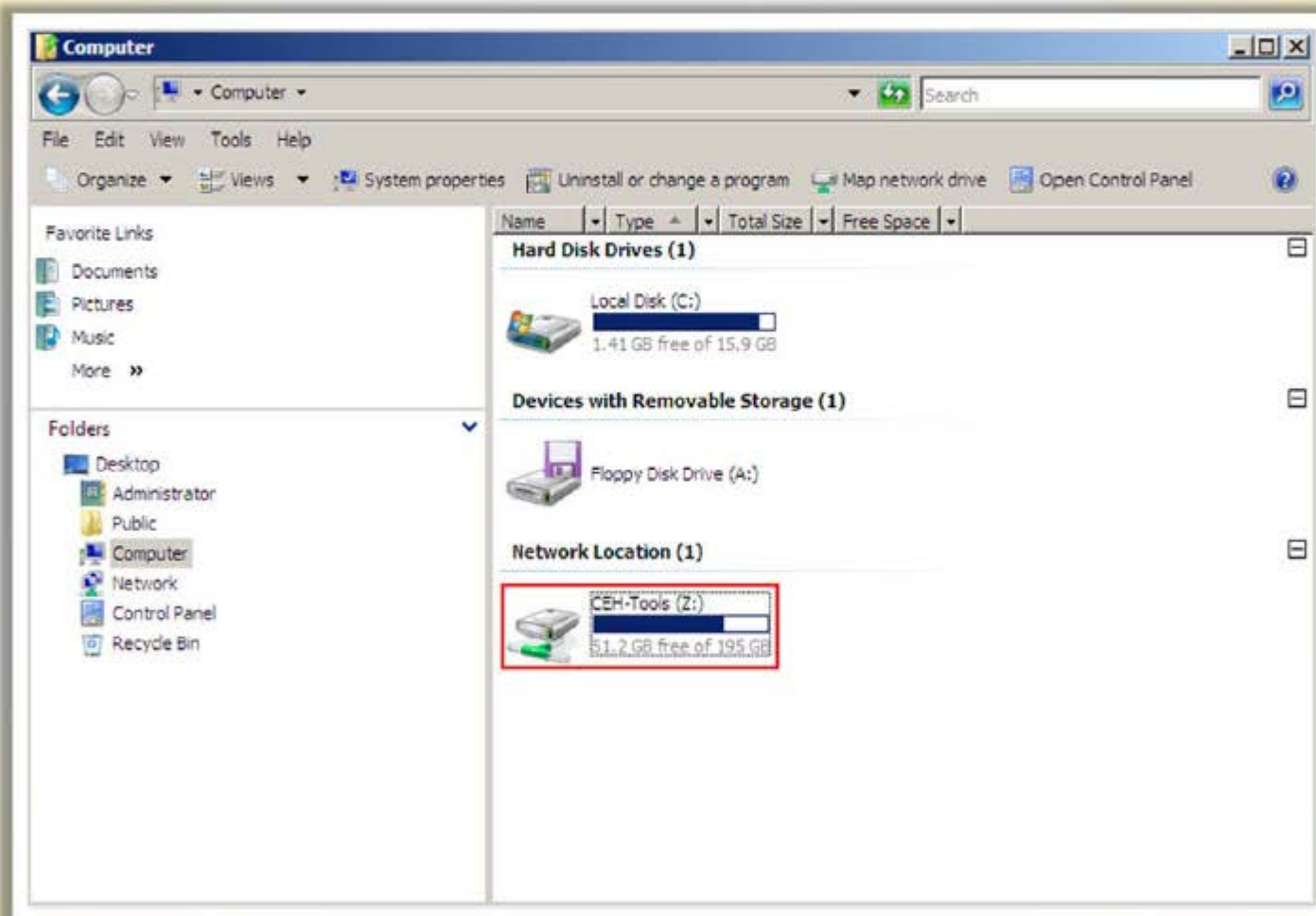
Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Mapped Network Drive (Z:) in Windows 8.1 VM



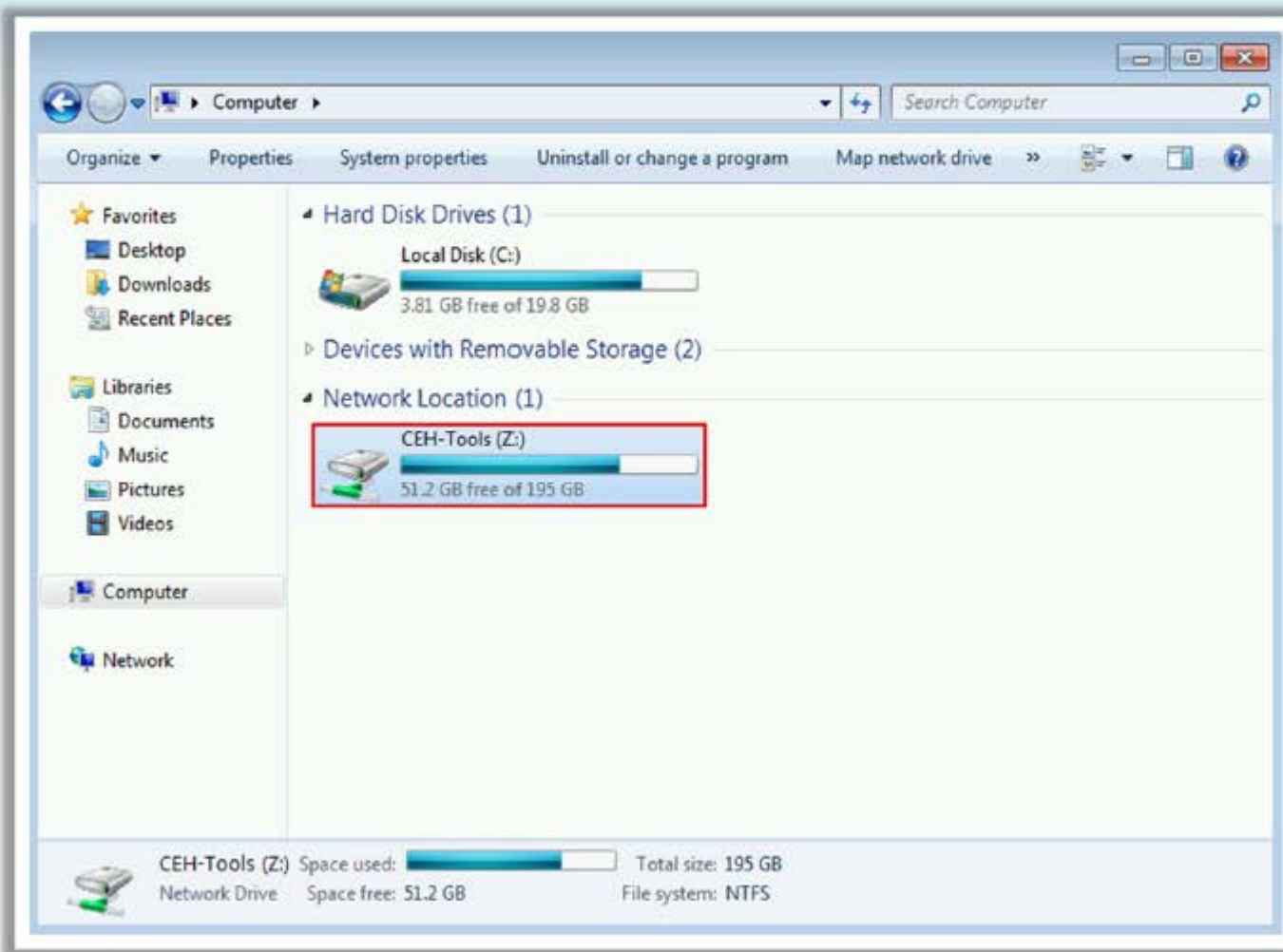
Copyright © by **EG-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Mapped Network Drive (Z:) in Windows Server 2008 VM

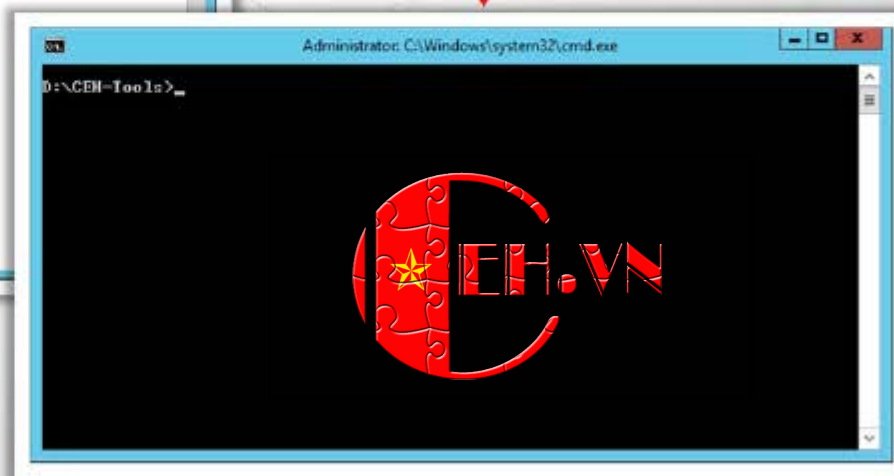
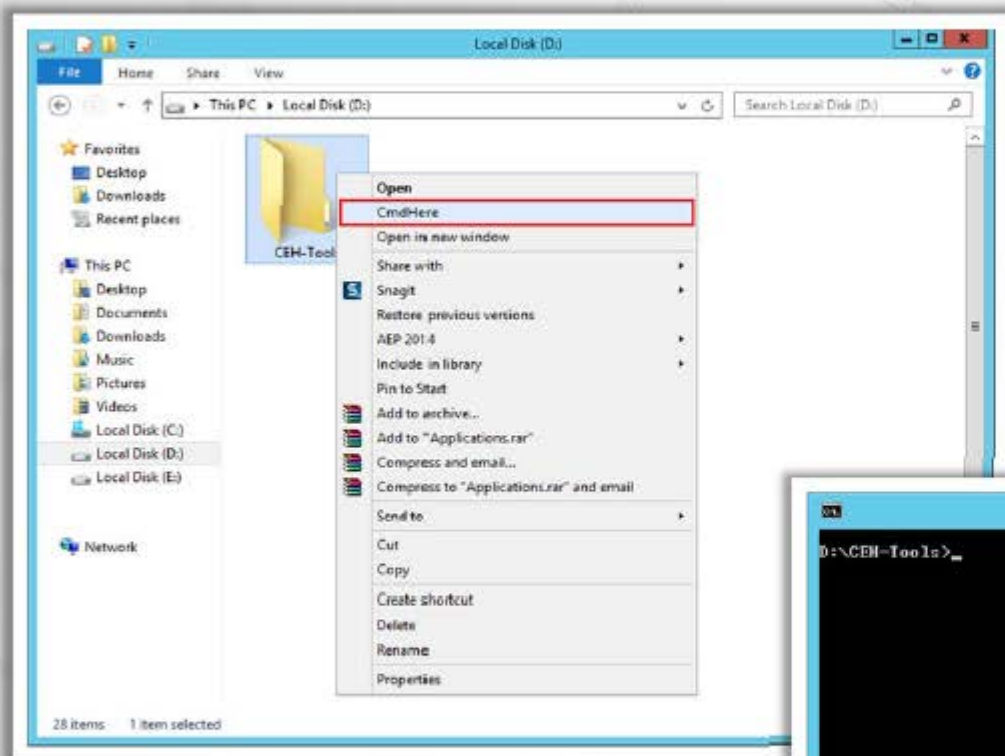


Copyright © by **EG-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

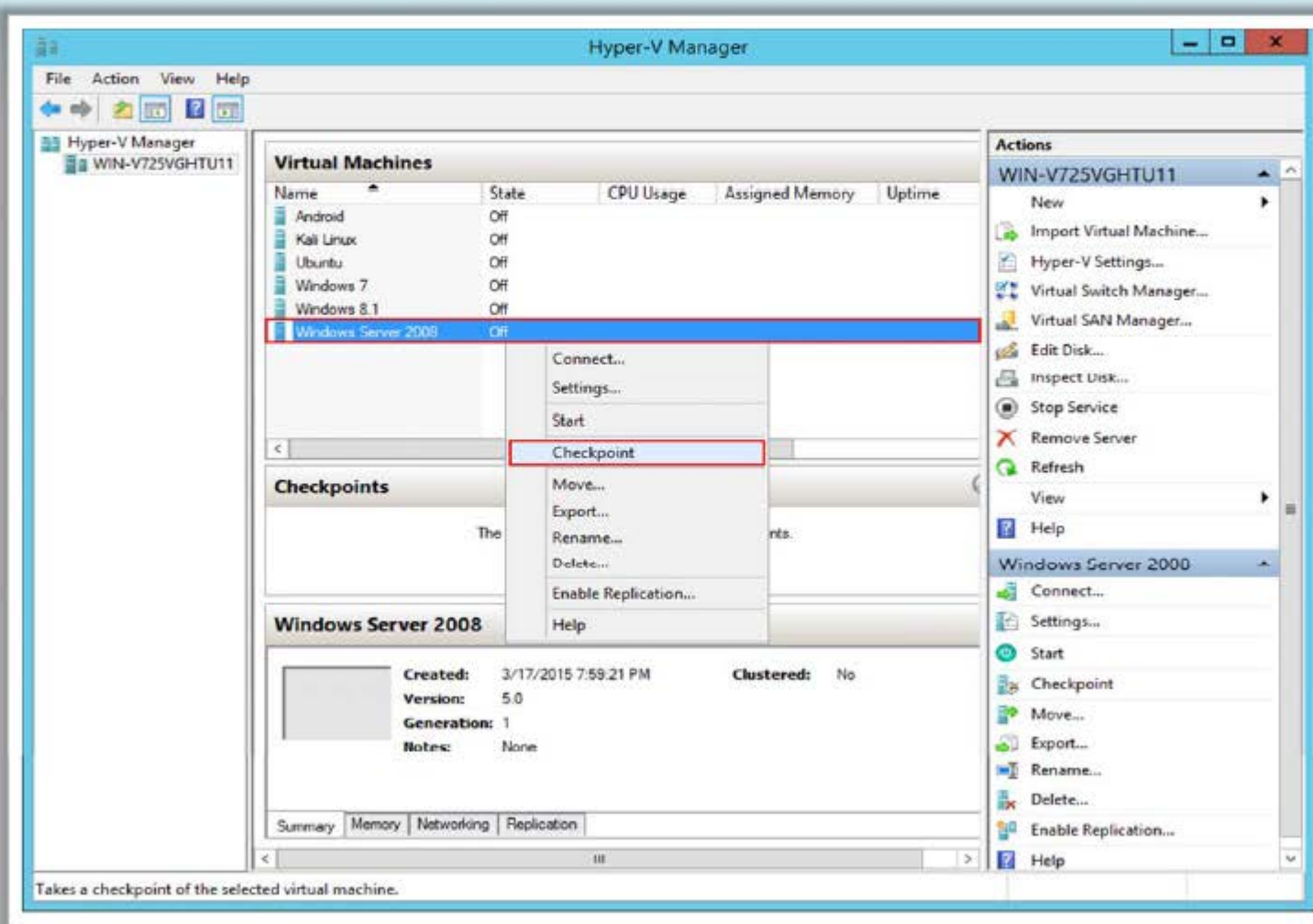
Mapped Network Drive (Z:) in Windows 7 VM



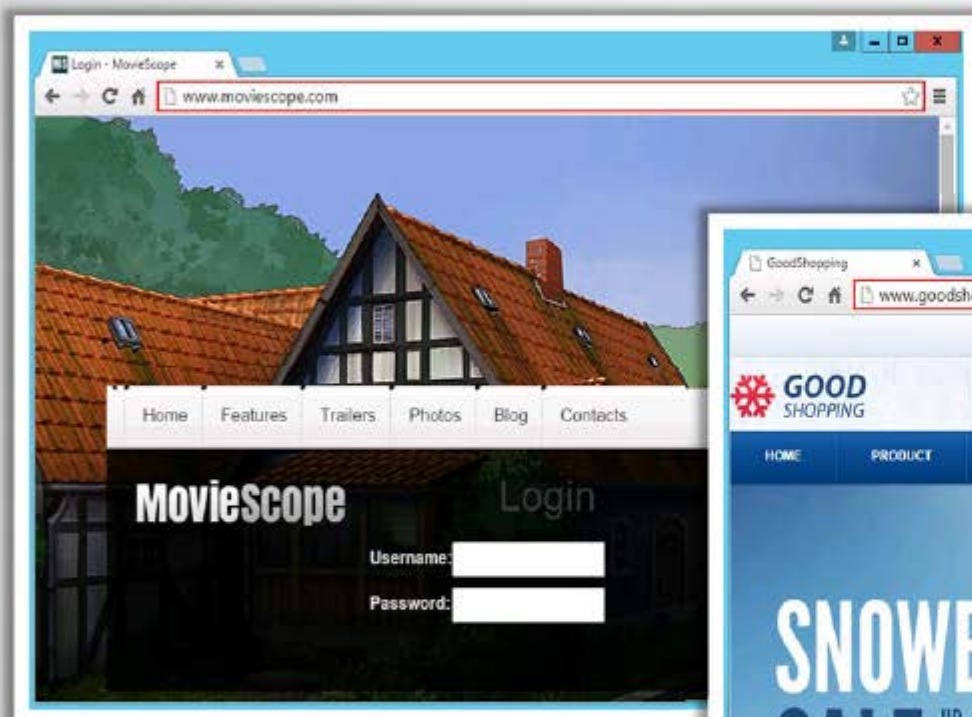
Launching Command Shell



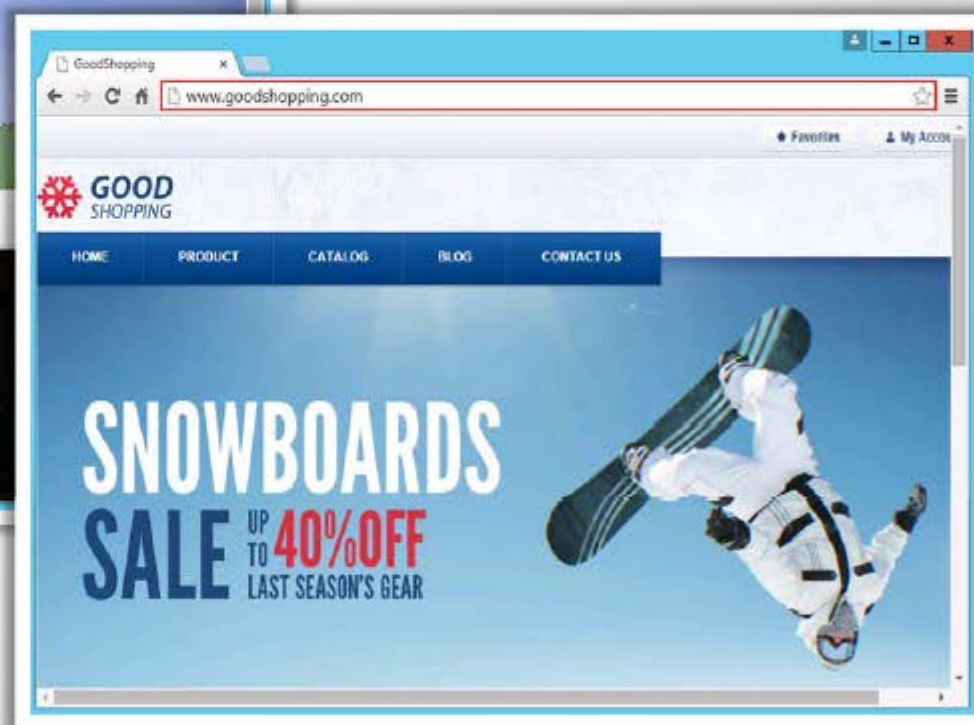
Checkpoints of Virtual Machines



Moviescope and GoodShopping Websites



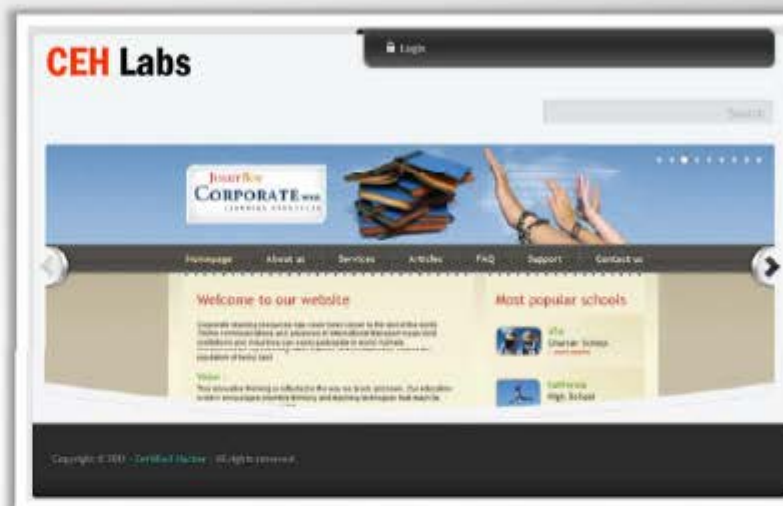
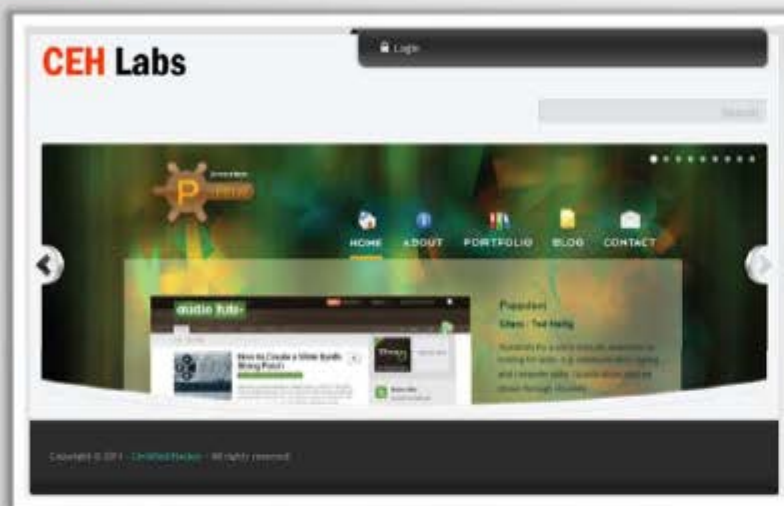
Moviescope: <http://www.moviescope.com>



GoodShopping: <http://www.goodshopping.com>

Live Hack Website

<http://www.certifiedhacker.com>



Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.



Let's Start **Hacking!**

