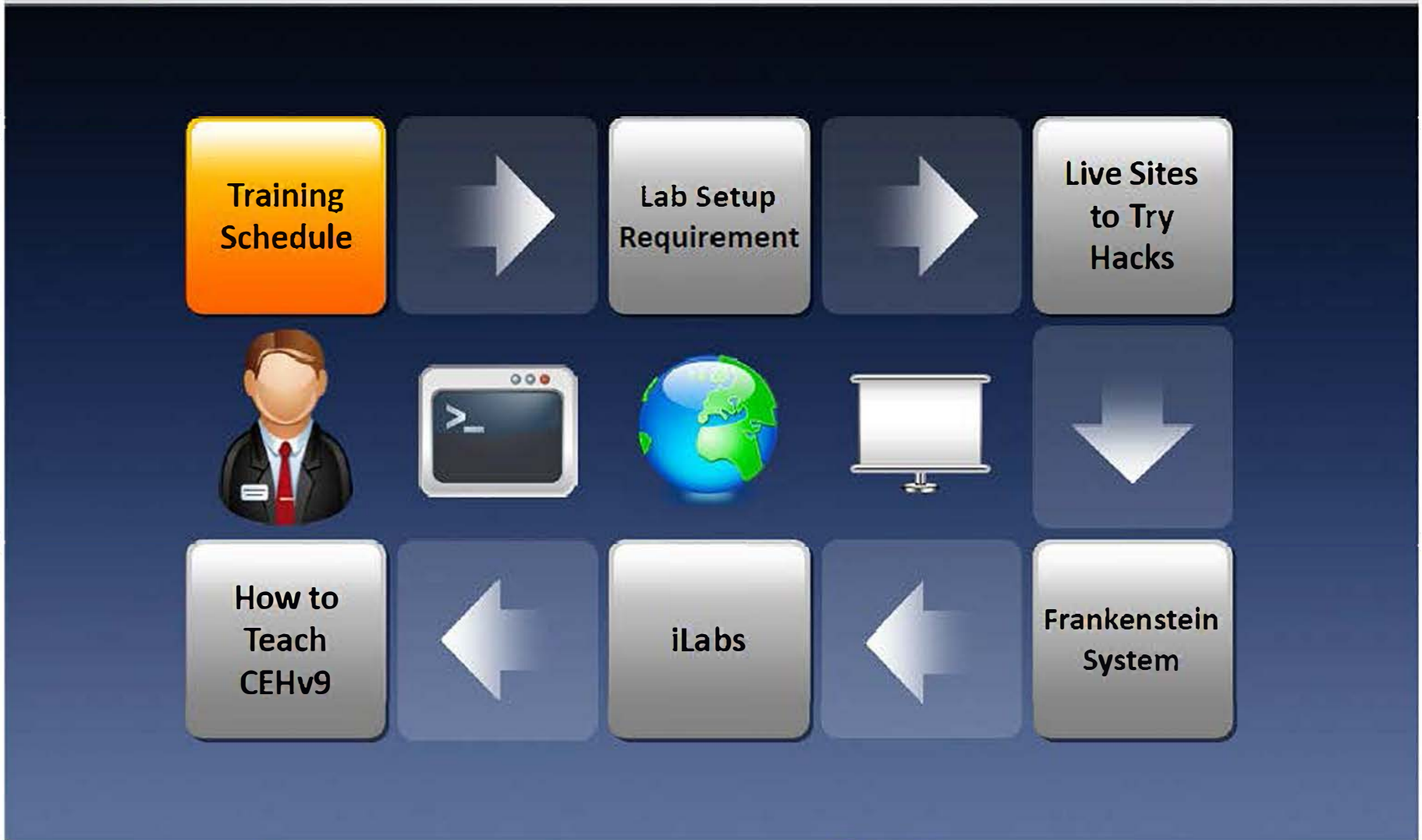
Content Flow



HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wEr FrEE t0 FlY
HaCkRhInO-TeaM !

Training Information

C|EH Certified Ethical Hacker

- Title of the Course: Ethical Hacking and Countermeasures
- Version: 9
- Training Duration: 5 Days
- Training Timing: 9:00 AM to 5:00 PM

Note: The CEHv9 is an advanced security training program. Proper preparation is required before conducting the CEH class.

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wEr FrEE t0 FIY
HaCkRhInO-TeaM !

Training Session: Day 1

Start	End	Module
9:00	9:15	Module 00: Student Introduction
9:15	10:45	Module 01: Introduction to Ethical Hacking
10:45	11:00	Break
11:00	12:30	Module 02: Footprinting and Reconnaissance
12:30	1:30	Lunch Break
1:30	2:45	Module 03: Scanning Networks
2:45	3:15	Break
3:15	5:00	Module 04: Enumeration

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wEr FrEE t0 FIY
HaCkRhInO-TeaM !

Training Session: Day 2

Start	End	Module
9:00	10:45	Module 05: System Hacking
10:45	11:00	Break
11:00	12:30	Module 05: System Hacking
12:30	1:30	Lunch Break
1:30	2:45	Module 06: Malware Threats
2:45	3:15	Break
3:15	5:00	Module 06: Malware Threats

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wEr FrEE t0 FIY
HaCkRhInO-TeaM !

Training Session: Day 3

Start	End	Module
9:00	10:45	Module 07: Sniffing Module 08: Social Engineering
10:45	11:00	Break
11:00	12:30	Module 09: Denial-of-Service
12:30	1:30	Lunch Break
1:30	2:45	Module 10: Session Hijacking
2:45	3:15	Break
3:15	5:00	Module 11: Hacking Webservers

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wEr FrEE t0 FIY
HaCkRhInO-TeaM !

Training Session: Day 4

Start	End	Module
9:00	10:45	Module 12: Hacking Web Applications
10:45	11:00	Break
11:00	12:30	Module 12: Hacking Web Applications
12:30	1:30	Lunch Break
1:30	2:45	Module 13: SQL Injection
2:45	3:15	Break
3:15	5:00	Module 14: Hacking Wireless Networks

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wEr FrEE t0 FIY
HaCkRhInO-TeaM !

Training Session: Day 5

Start	End	Module
9:00	10:45	Module 15: Hacking Mobile Platforms
10:45	11:00	Break
11:00	12:30	Module 16: Evading IDS, Firewalls, and Honeypots
12:30	1:30	Lunch Break
1:30	2:45	Module 17: Cloud Computing
2:45	3:15	Break
3:15	5:00	Module 18: Cryptography

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wEr FrEE t0 FlY
HaCkRhInO-TeaM !

Instructors may alter the structure of the course and the timings to meet their requirements.

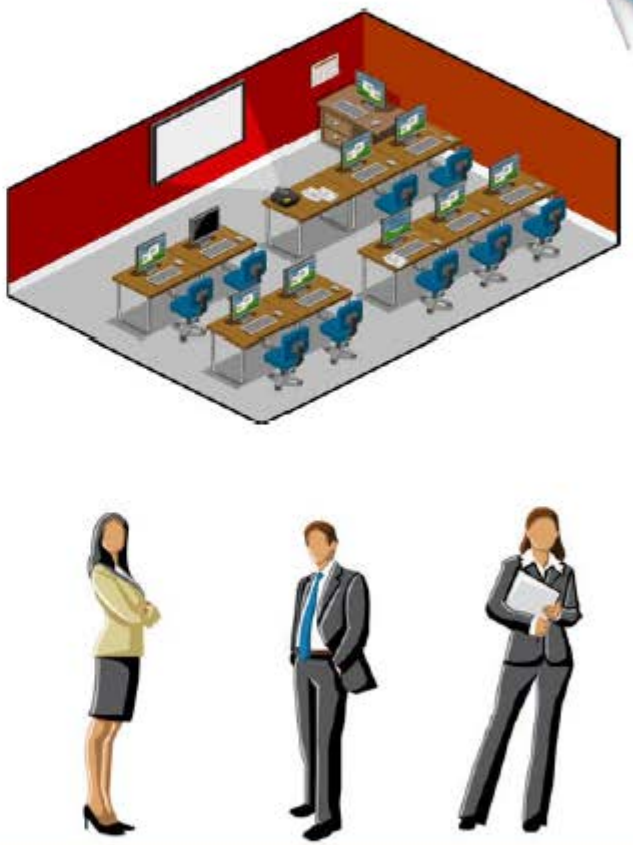
HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wEr FrEE t0 FIY
HaCkRhInO-TeaM !

Content Flow

Minimum System Requirements

C|EH Certified Ethical Hacker

- **Intel Dual Core PC** with 100 GB free disk space
- **8 GB RAM**
- **1 NIC** (disable or unplug extras)
- **15-inch monitor** and VGA cards to drive at 1024 x 768 (or at monitor's native resolution) and configured at 16 million colors
- Compatible **keyboard** and **mouse**
- **Wireless Card** for Wi-Fi access (Kali Linux compatible wireless card for Wireless hacking demonstration on Kali Linux)



Basic Lab Setup Requirements

1. Windows Server 2012 with full patches and hot fixes applied
2. MS SQL Server 2012
3. MS Internet Information Server 7.0 (IIS 7.0) or later
4. SNMP Services
5. Microsoft .NET Framework 4.5 SP1 or higher version
6. Adobe Acrobat Reader 11 or later version
7. WinRAR 4.20 or later version

Basic Lab Setup Requirements

- Web Browsers: Internet Explorer, Firefox, Chrome, Safari, and Opera
- AirPcap adapter and driver for Wi-Fi packet capturing demonstrations
- WinPcap driver
- Notepad++
- Cmdhere script
- Active Perl 5 or later version
- Word, Excel, and PowerPoint Viewers

Basic Lab Setup Requirements

Hyper-V (Built-in role in Windows Server 2012)

Microsoft Windows 8.1 with full patches and hot fixes applied

Microsoft Windows Server 2008 with full patches and hot fixes applied

Microsoft Windows 7 with full patches and hot fixes applied

Kali Linux (from CEH DVDs Pack) with full patches and hot fixes applied

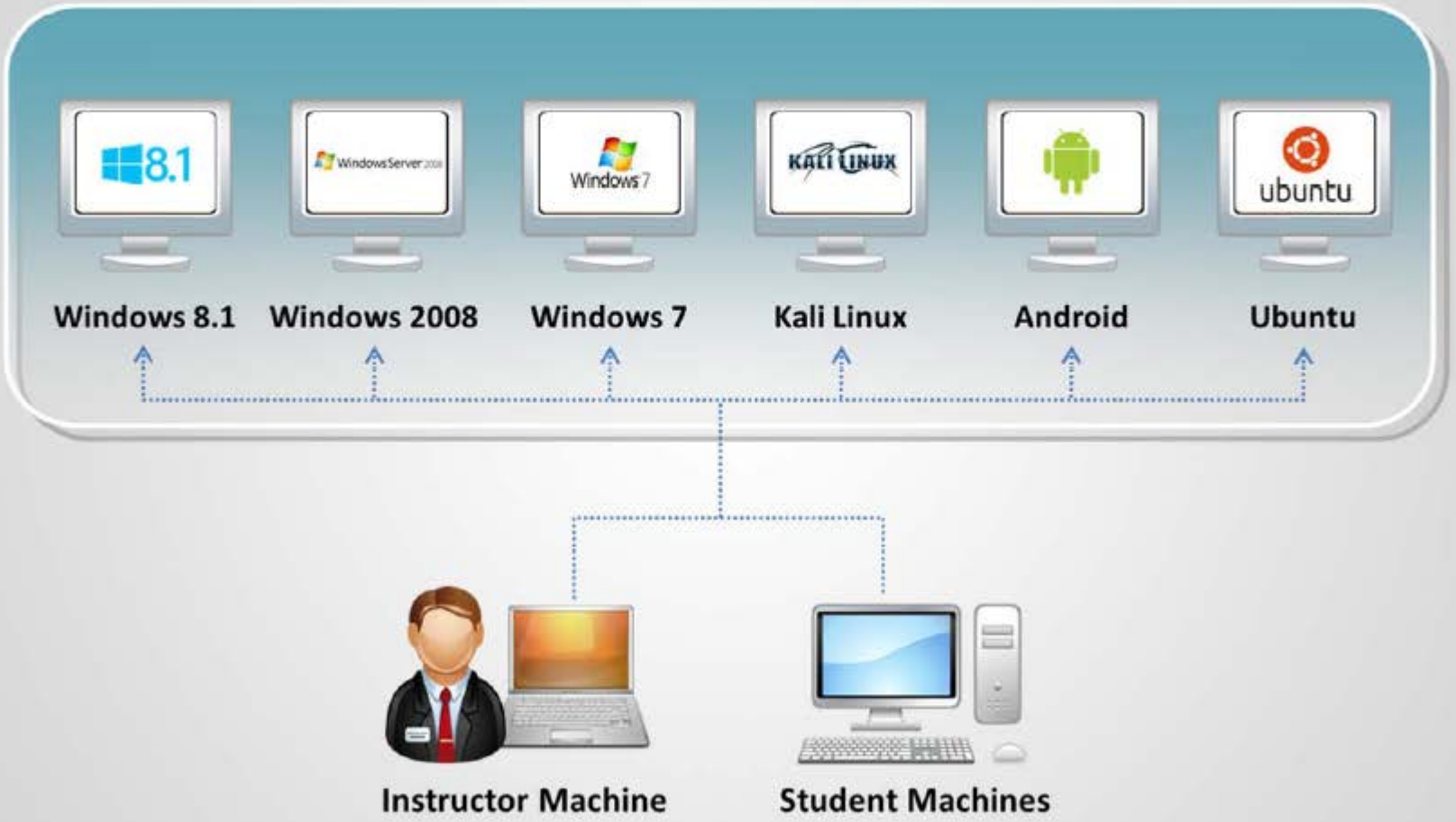
Android (from CEH DVDs Pack) with full patches and hot fixes applied

Ubuntu (from CEH DVDs Pack) with full patches and hot fixes applied

Note: Please check the Lab Setup Guide available in Instructors Area at www.eccouncil.org for detailed lab setup instructions

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wEr FrEE t0 FIY
HaCkRhInO-TeaM !

Instructor and Student Virtual Machine Operating System



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

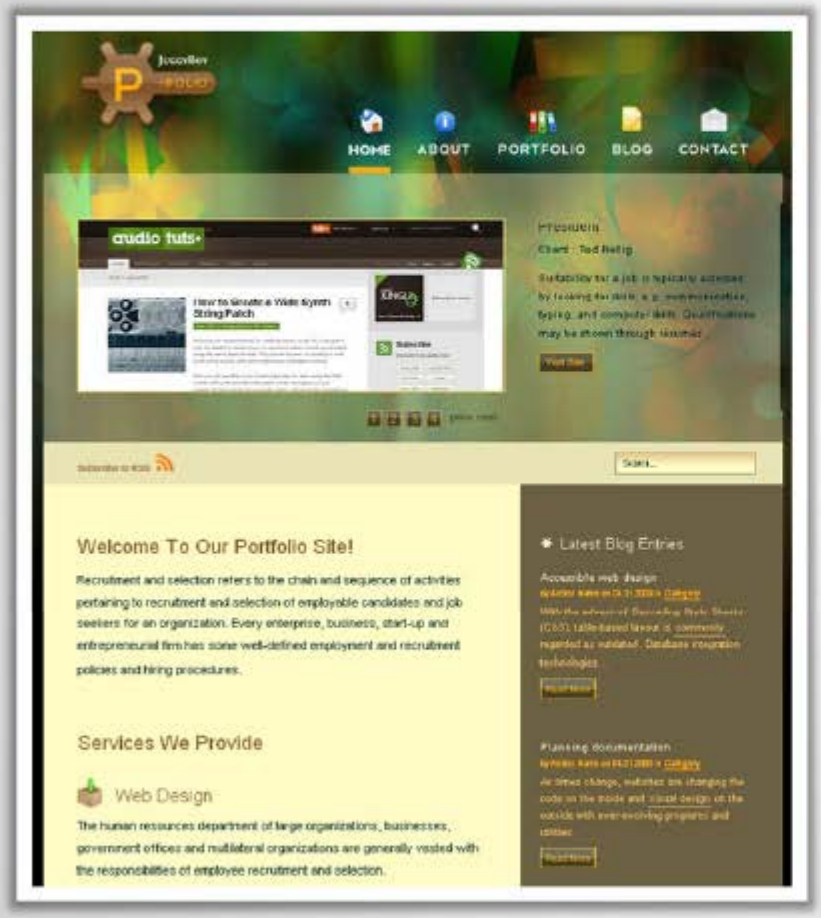
HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wEr FrEE t0 FIY
HaCkRhInO-TeaM !

Content Flow

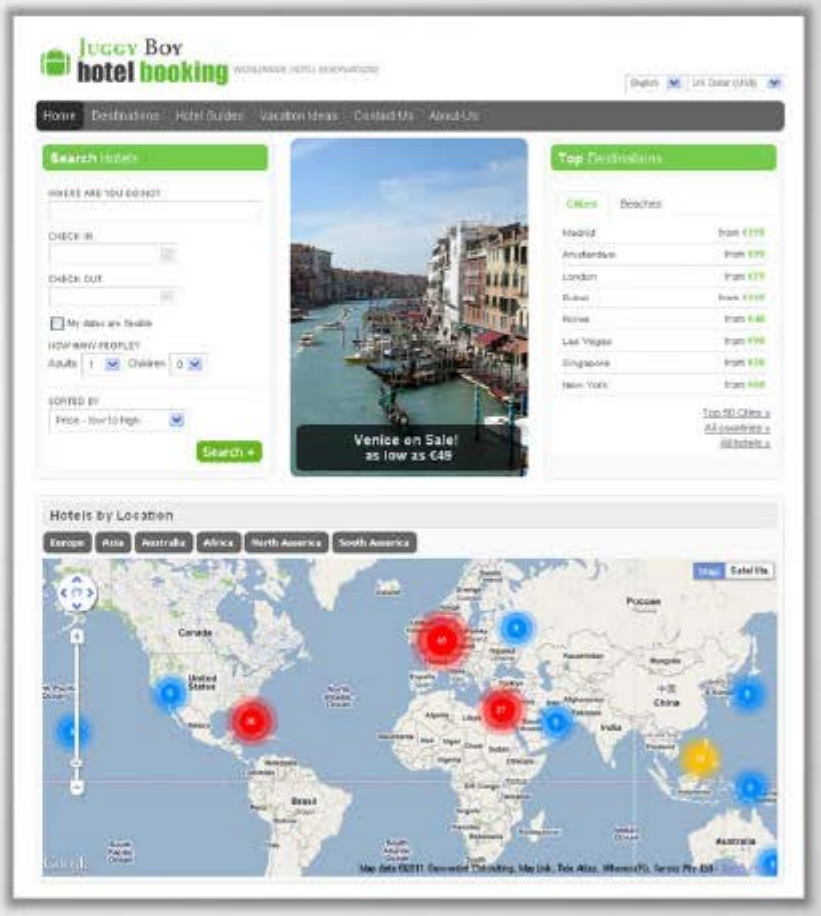
HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wEr FrEE t0 FIY
HaCkRhInO-TeaM !

Live Sites to Try Hacks

C|EH Certified Ethical Hacker



http://certifiedhacker.com/P-folio



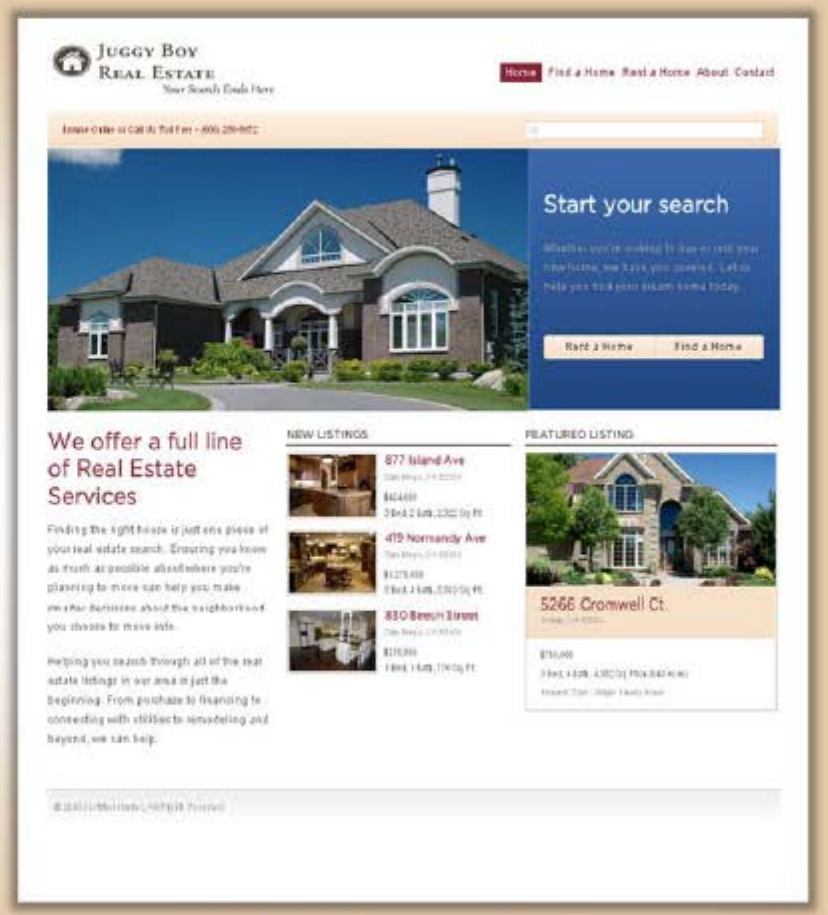
http://certifiedhacker.com/Online Booking

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wEr FrEE t0 FIY
HaCkRhInO-TeaM !

Live Sites to Try Hacks

C|EH Certified Ethical Hacker

http://certifiedhacker.com/corporate-learning-website/01-homepage.html

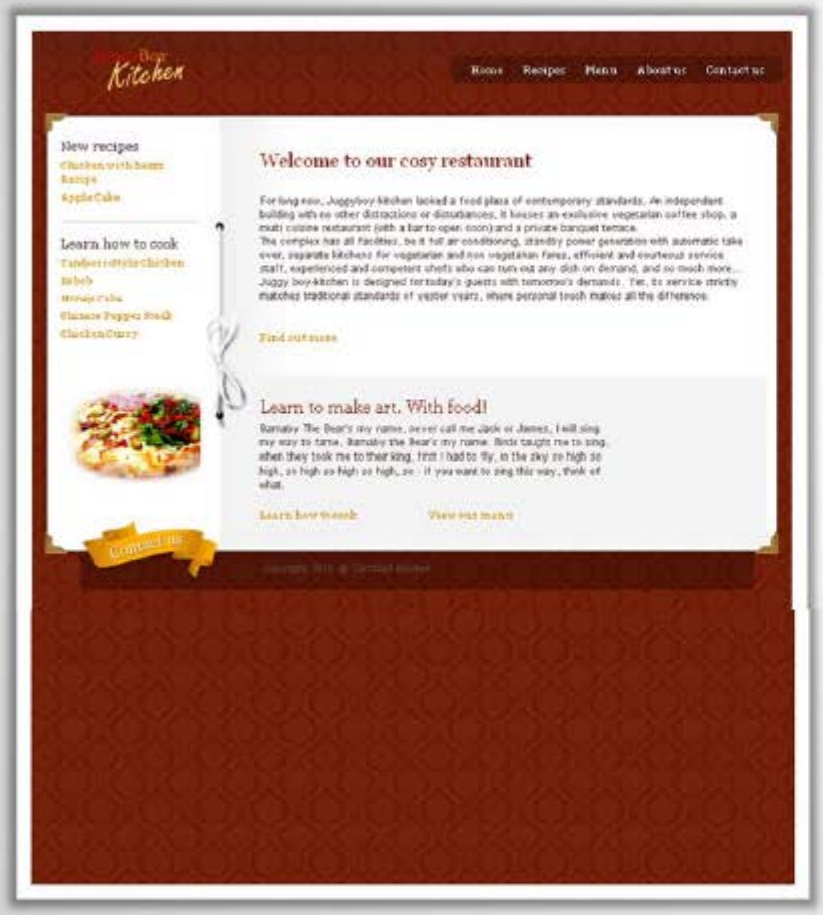


http://certifiedhacker.com/Real Estates

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wEr FrEE t0 FIY
HaCkRhInO-TeaM !

Live Sites to Try Hacks

C|EH Certified Ethical Hacker



http://certifiedhacker.com/Recipes

http://certifiedhacker.com/Social Media

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wEr FrEE t0 FIY
HaCkRhInO-TeaM !

Live Sites to Try Hacks

C|EH Certified Ethical Hacker

http://certifiedhacker.com/Turbo Max

http://certifiedhacker.com/Under the trees

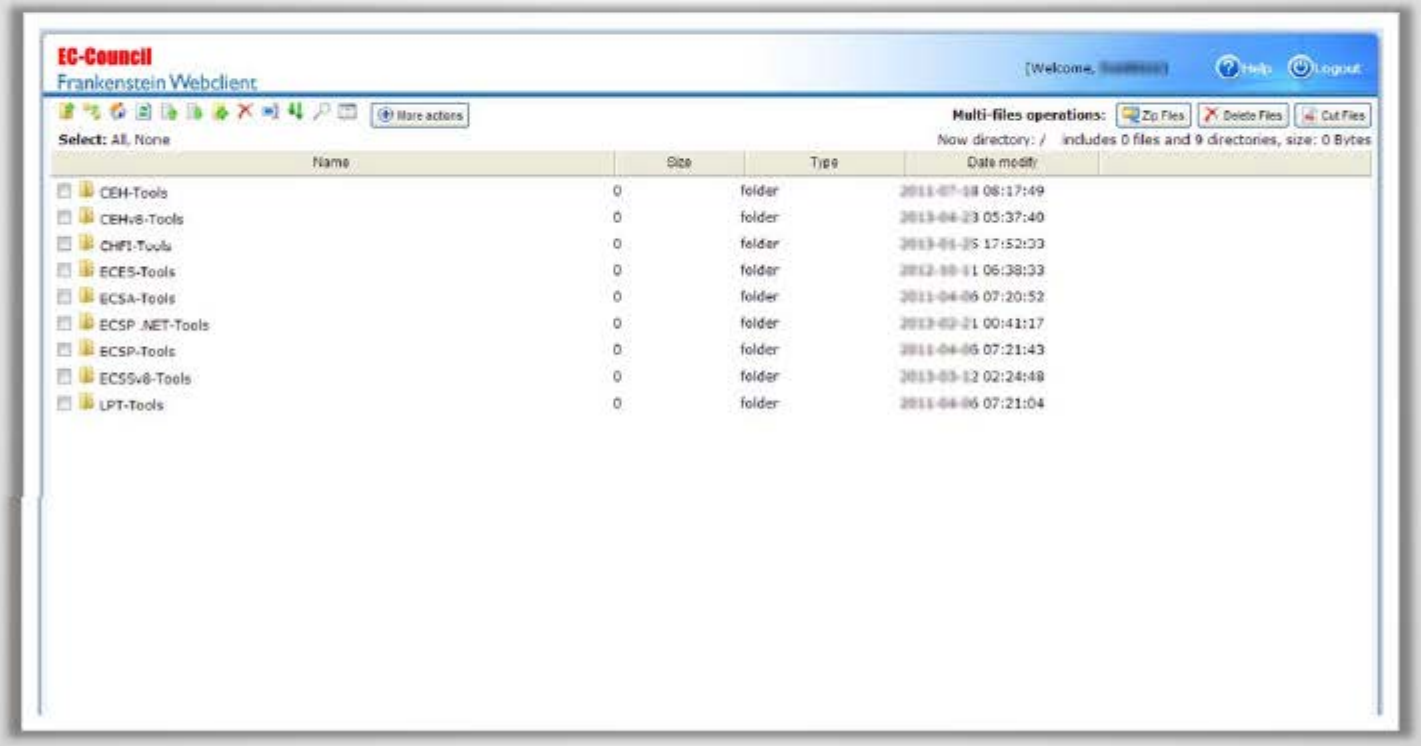
HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wEr FrEE t0 FIY
HaCkRhInO-TeaM !

Content Flow

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wEr FrEE t0 FIY
HaCkRhInO-TeaM !

What is Frankenstein?

- Frankenstein is designed to provide user with an ease for **Searching**, **Downloading**, and **Installing** the tools
- Frankenstein Server's Web Client:
  - Web Client is a web application that allows you to access or share files merely by a standard web browser
  - It is simple and very useful. With it you can connect to the server from a local area network (LAN) or a wide area network (WAN)



HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wEr FrEE t0 FIY
HaCkRhInO-TeaM !

Why it is Made?

To provide a repository of categorized latest tools

User can download the tool in less time with comparison to manual search

It will help the user to synchronize and manage the tools

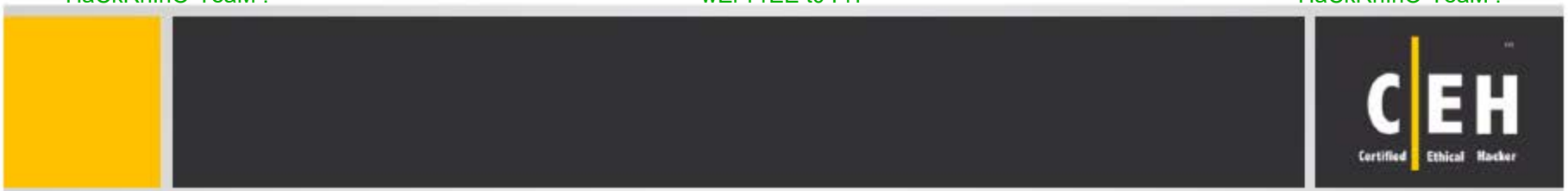
User can search the tools from the available list of tools

The system provides a means to generate a HTML report of all the tools downloaded by the user

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wEr FrEE t0 FIY
HaCkRhInO-TeaM !

Features

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wEr FrEE t0 FIY
HaCkRhInO-TeaM !



Please download Frankenstein tools at

https://frank.eccouncil.org/

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wEr FrEE t0 FIY
HaCkRhInO-TeaM !

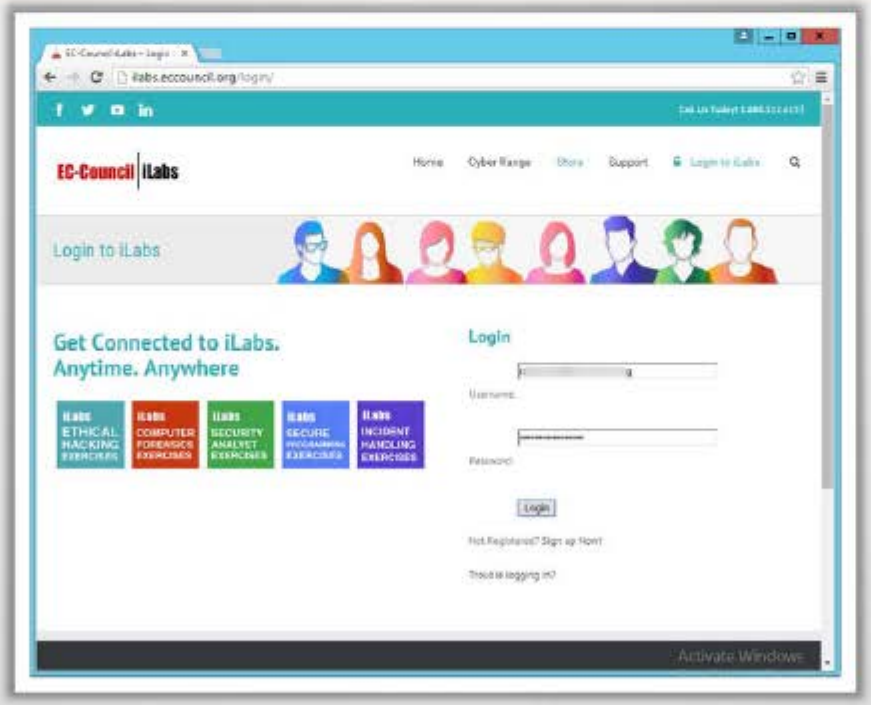
Content Flow

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wEr FrEE t0 FIY
HaCkRhInO-TeaM !

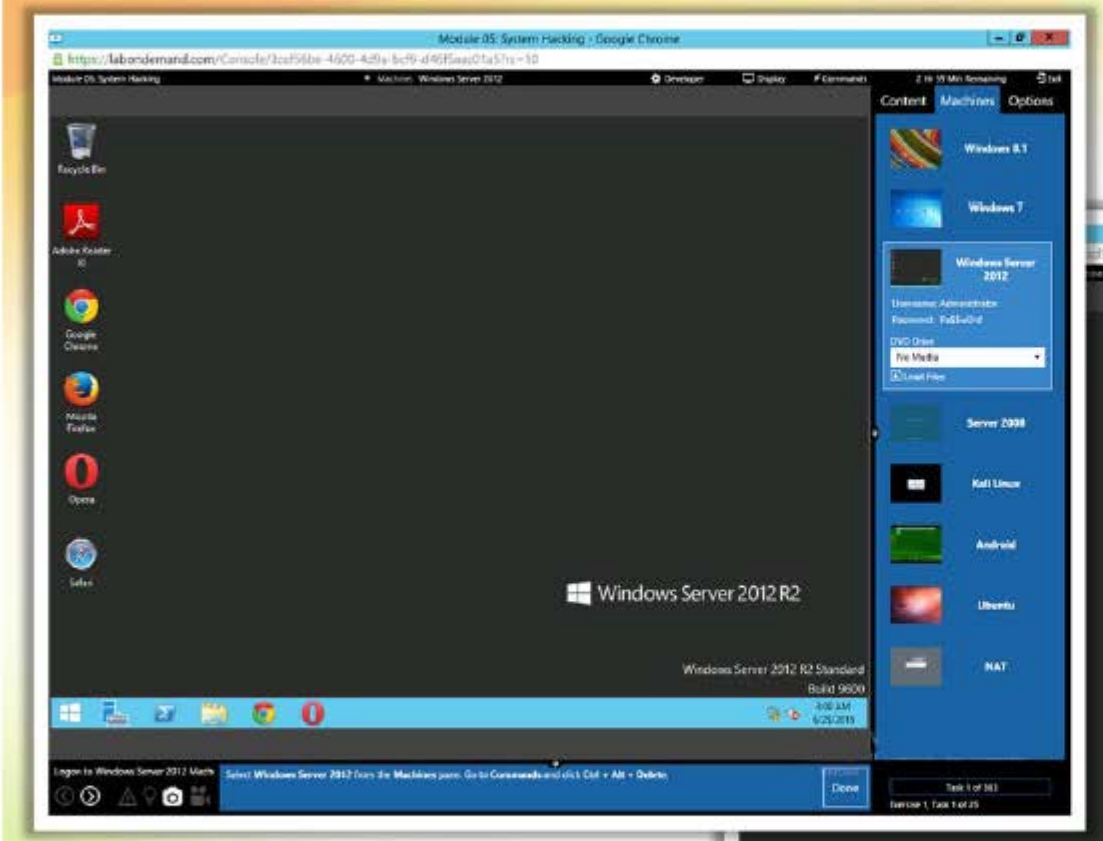
EC-Council iLabs

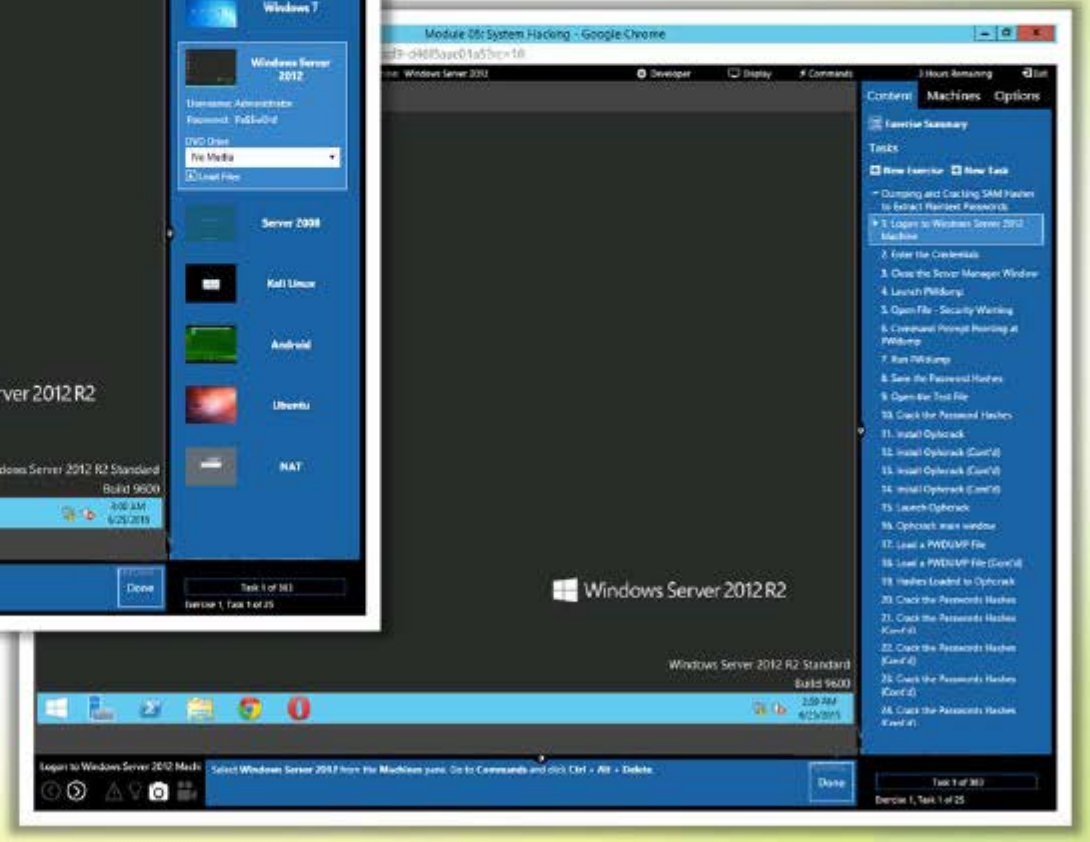
C|EH Certified Ethical Hacker

The iLabs is a subscription based service that allows students to logon to a virtualized remote machine running Windows Server 2012 to perform various exercises featured in the CEHv9 Lab Guide



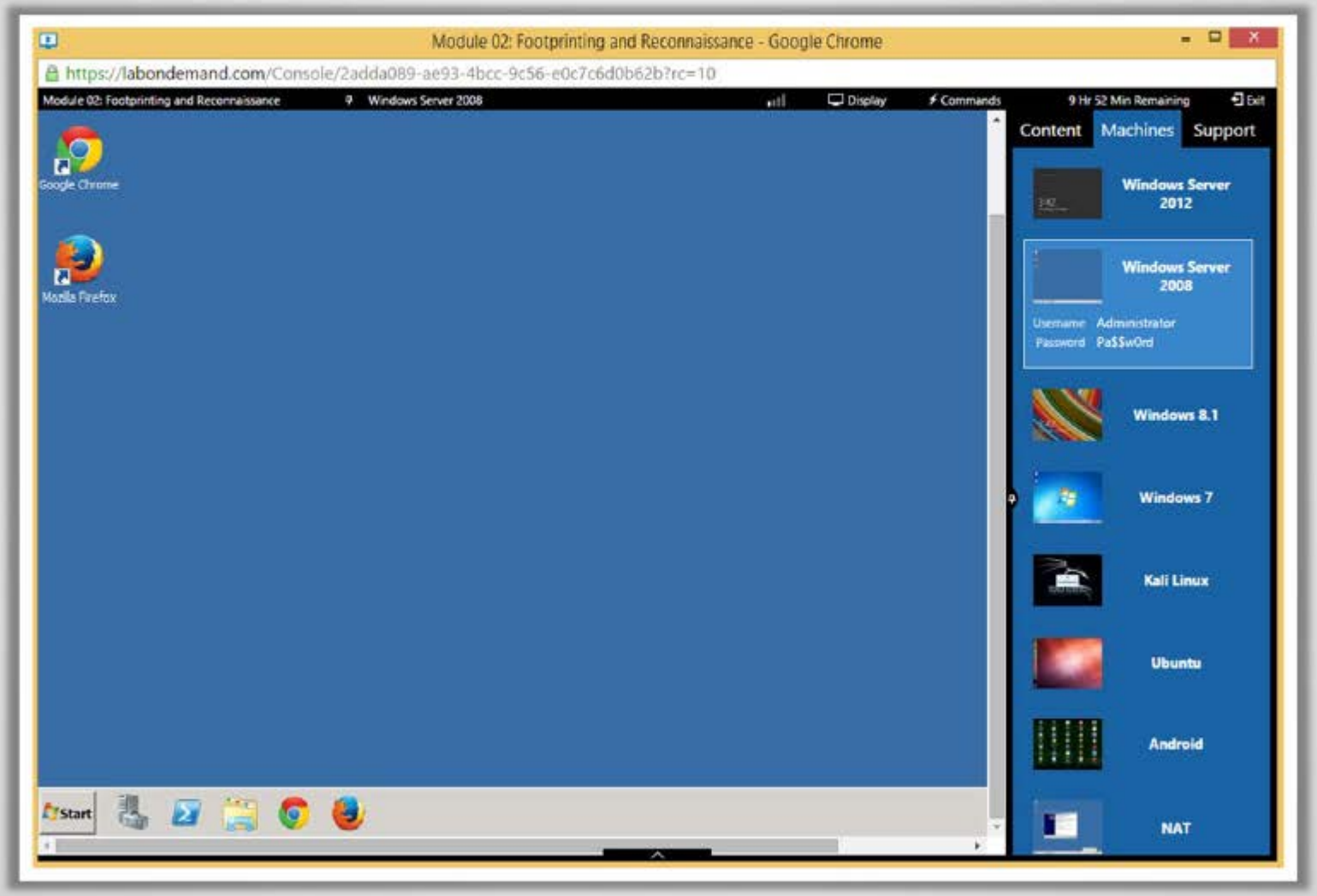
Windows Server 2012 Primary Control Machine





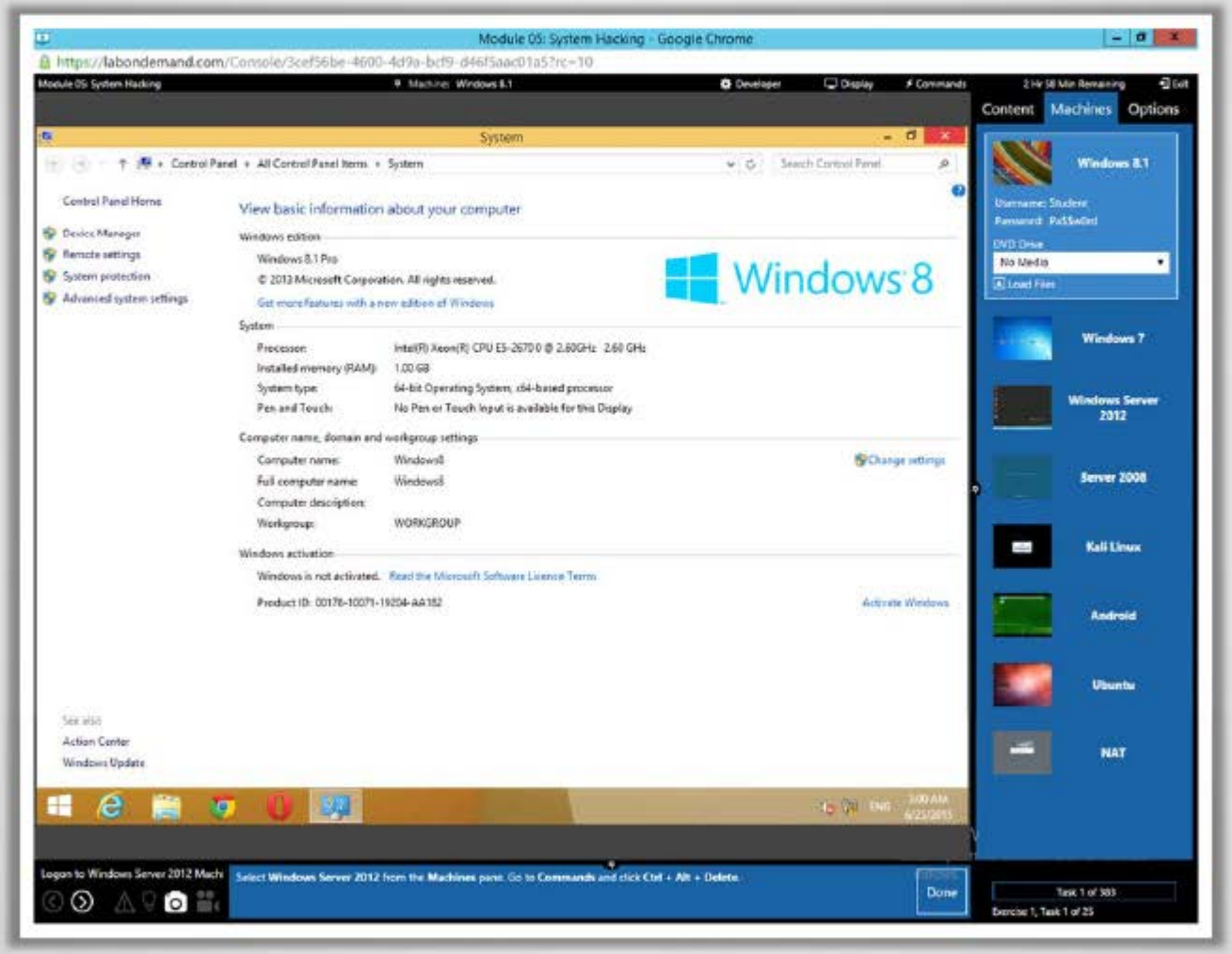
HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wEr FrEE t0 FIY
HaCkRhInO-TeaM !

Windows Server 2008 Secondary Machine



HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wEr FrEE t0 FIY
HaCkRhInO-TeaM !

Windows 8.1 Secondary Machine

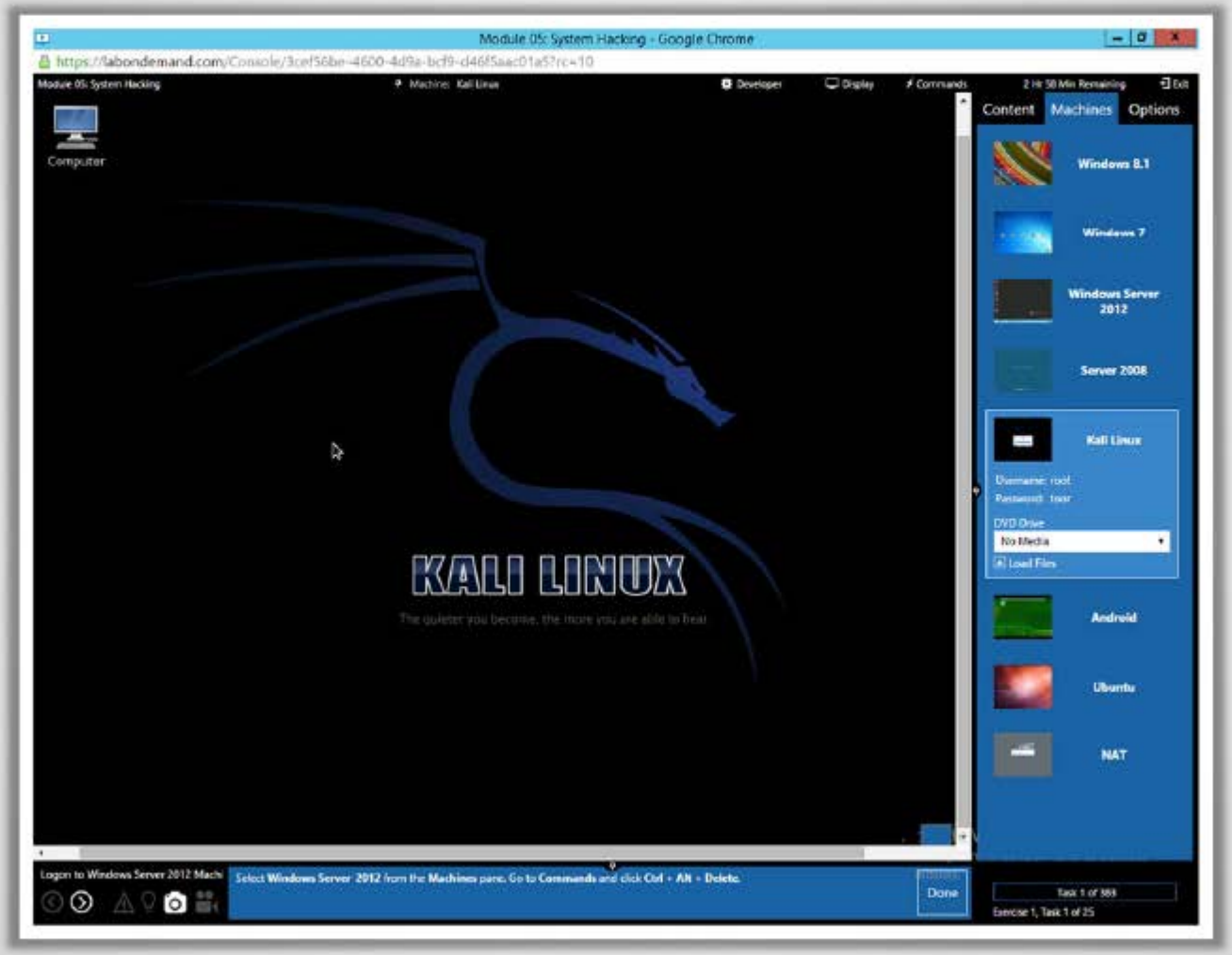


HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wEr FrEE t0 FIY
HaCkRhInO-TeaM !

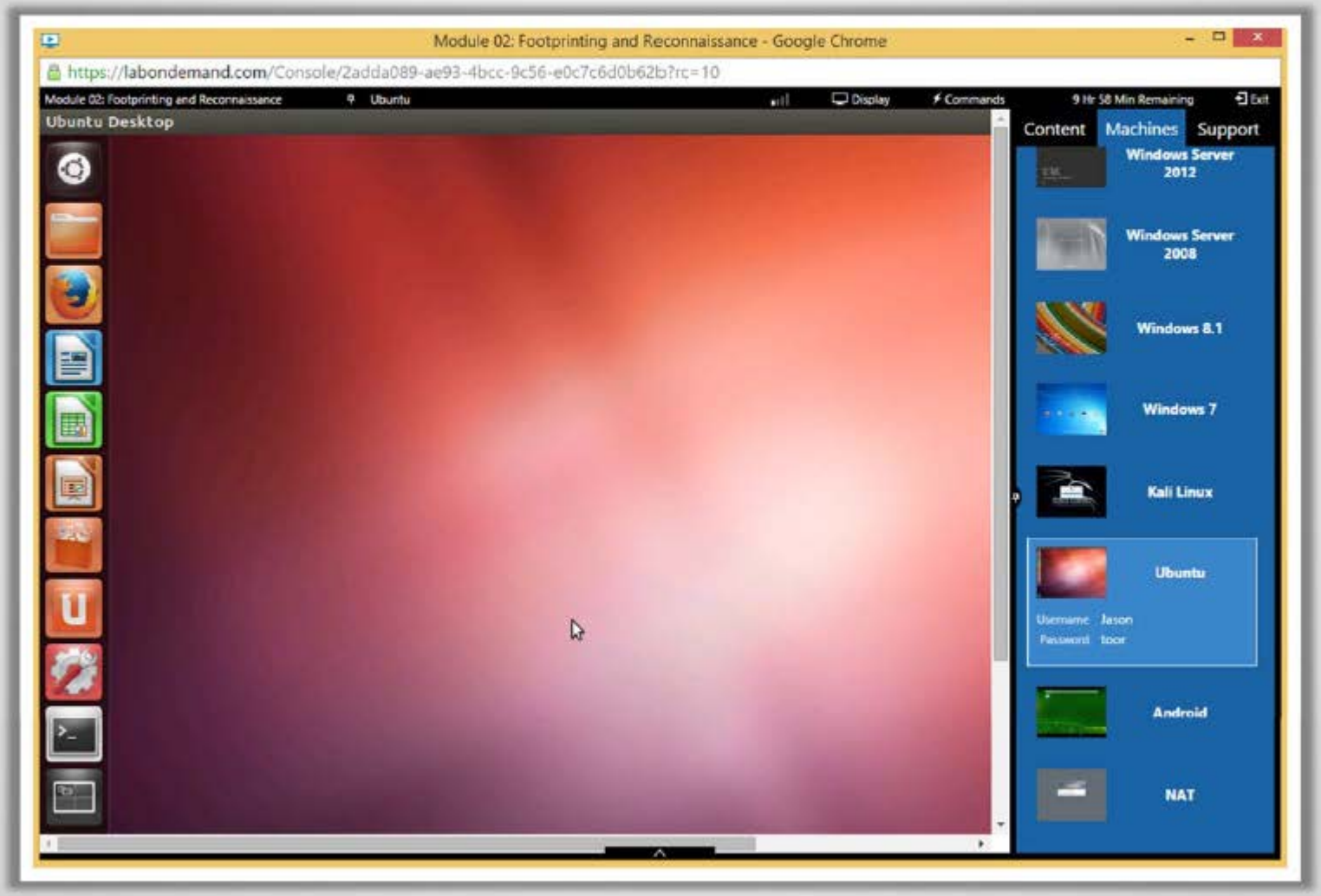
Windows 7 Secondary Machine

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wEr FrEE t0 FIY
HaCkRhInO-TeaM !

Kali Linux Secondary Machine

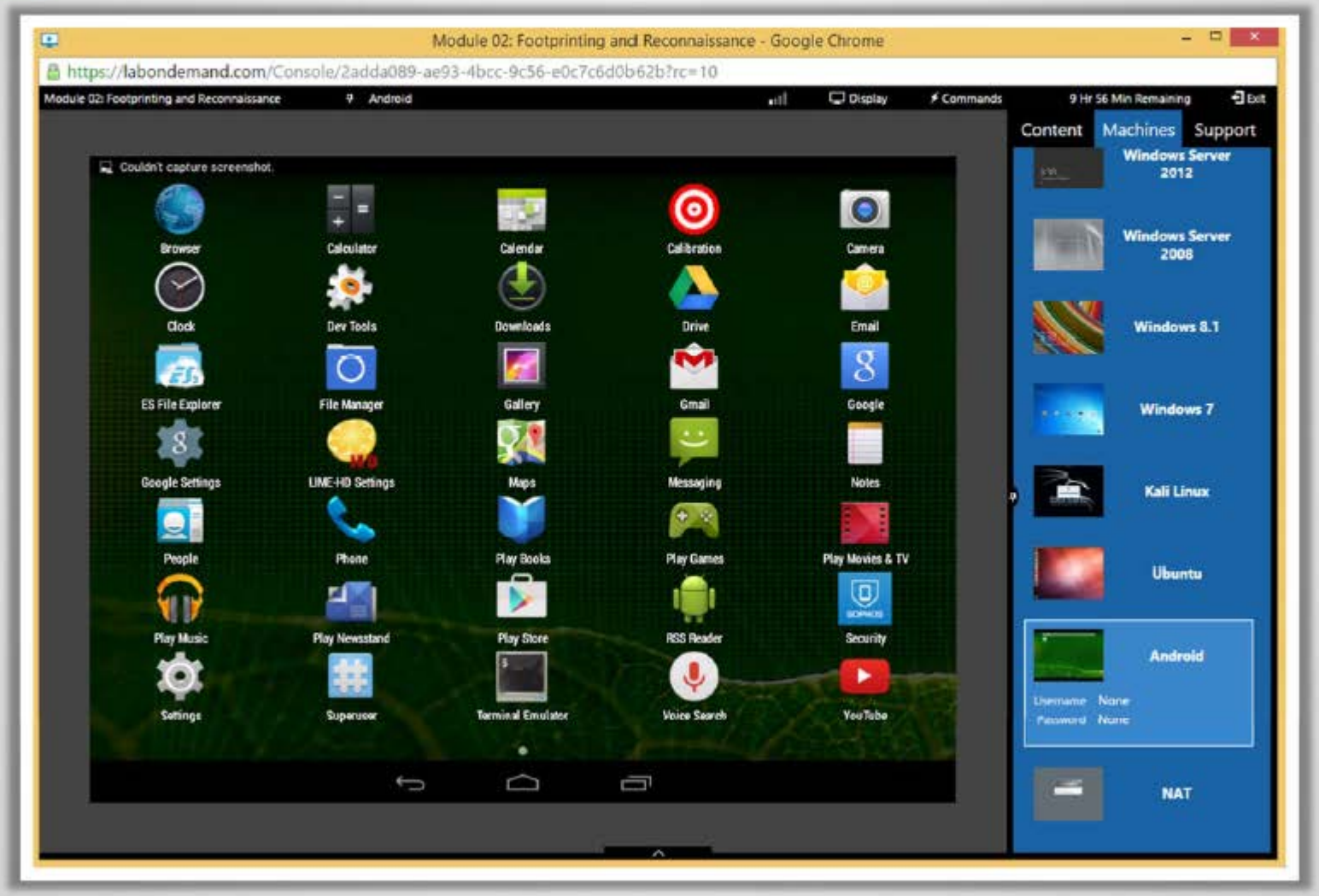


Ubuntu Secondary Machine



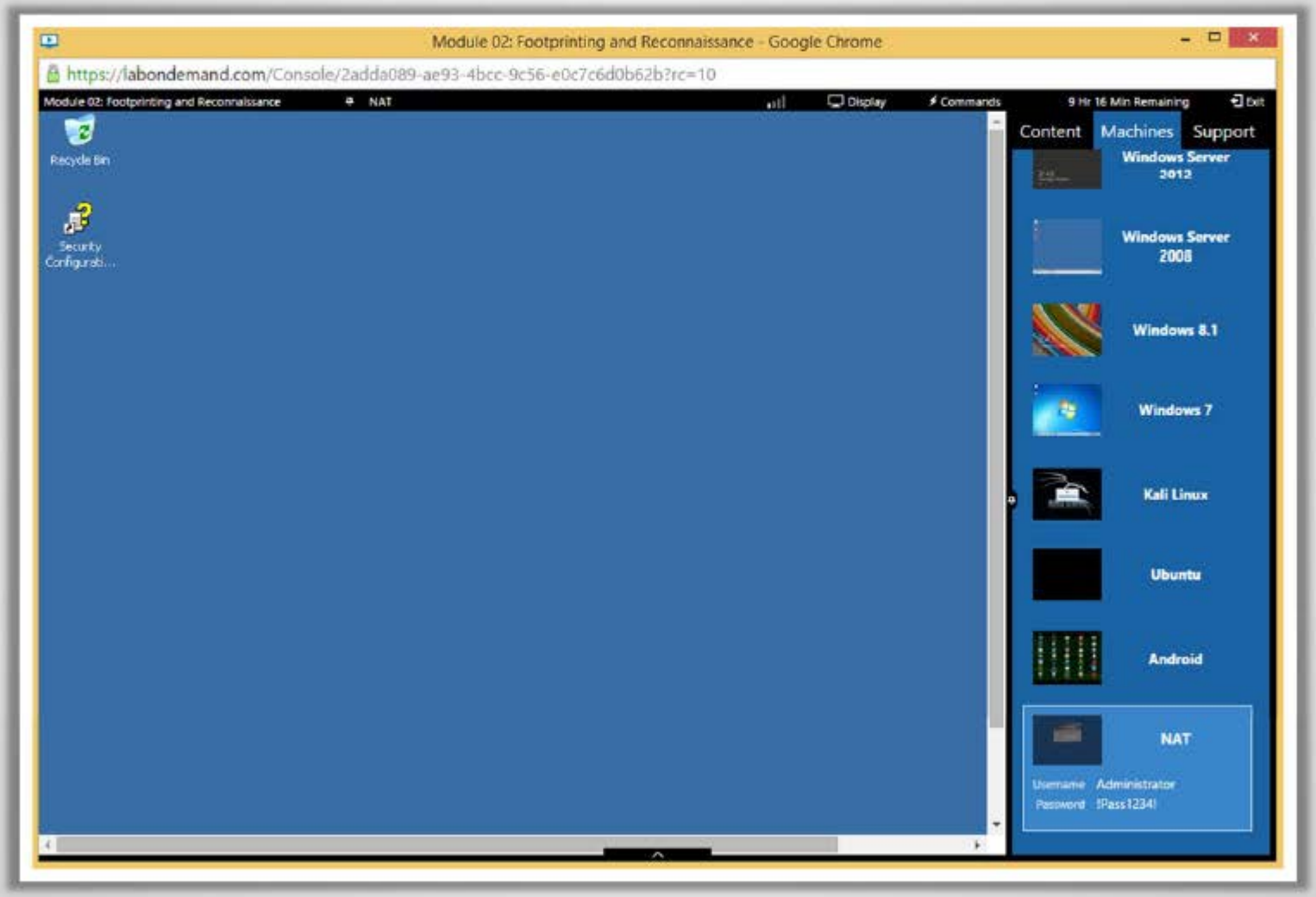
HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wEr FrEE t0 FIY
HaCkRhInO-TeaM !

Android Secondary Machine



HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wEr FrEE t0 FIY
HaCkRhInO-TeaM !

NAT Secondary Machine



HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wEr FrEE t0 FIY
HaCkRhInO-TeaM !

EC-Council iLabs Benefits

C|EH Certified Ethical Hacker

Student Benefits

- Fully Automated Lab Environment
- Unlimited Access over Subscription Term
- Simple clientless connection through web browser
- Fully loaded with Windows 8.1, Kali Linux, Windows Server 2012 64-bit, Windows Server 2008 64-bit, Windows 7, Ubuntu, and Android Operating Systems
- Save-State Technology enabled
- **Labs can be performed at HOME!**

Instructor/ATC Benefits

- No more difficult Lab Setup
- No Software licensing Fees
- No Hardware to maintain
- Full Controls to reset or re-spin systems live
- Instant recovery

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wEr FrEE t0 FIY
HaCkRhInO-TeaM !

Content Flow

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wEr FrEE t0 FIY
HaCkRhInO-TeaM !

Note to Instructors

Please note that this is a **proposed course structure** for the CEHv9 course.

While most instructors have their own style, this document is **meant to be a guide** from which instructors can understand EC-Council's vision.

Instructors **MUST be certified in the version 9** PRIOR to the delivery of the program.

Instructors must practice the labs before going to the class and must be **proficient in the usage of iLabs**.

Several labs in the **How to Teach This Module** slides are marked as **Self-Study**. While these labs are meant for students to practice on their own, instructors can select the labs from the available pool to demonstrate in the class based on student's skill level and availability of the time.

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wEr FrEE t0 FIY
HaCkRhInO-TeaM !

Module 00: Student Introduction

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wEr FrEE t0 FIY
HaCkRhInO-TeaM !

Student Introduction

C|EH Certified Ethical Hacker

Welcome the students to the course and introduce yourself

Provide a brief overview of your background to establish credibility

Ask students to introduce themselves and provide their background, security related experience, and expectations from the course

Ask the students if they have Linux and C++ programming experience

Write your name on the whiteboard corner and do not erase this for the duration of the class so that the students will know your name

Tell students everything that they will need for the CEH course and describe the contents of the CEH courseware and the contents of the DVD-ROM

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wEr FrEE t0 FIY
HaCkRhInO-TeaM !

Student Introduction

Tell the students about the modules that will be covered in the class and also explain them on the CEHv9 exam and the process of taking it

You can give information to the students on when the exam will be conducted, the cost of the exam, the total number of questions, the passing score, etc. (consult with the training center regarding the exam delivery, they might have a prepaid exam voucher)

Give them the link of the live website to hack for testing purposes in the class which is *http://www.certifiedhacker.com* (Write this information on the corner of the whiteboard)

Give EC-Council's CEH NDA document to the students for signing. After their signature hand them over to the training center operations manager or the person in charge of the training

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wEr FrEE t0 FIY
HaCkRhInO-TeaM !

Module 01: Introduction to Ethical Hacking

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wEr FrEE t0 FIY
HaCkRhInO-TeaM !

What is Covered in Module 01?

- The module briefs on **current security trends**, various elements of information security, and security challenges
- Discusses **information security threats** and attack vectors
- Discusses various **hacking concepts**, types, and phases
- Briefs about ethical hacking concepts and scope
- Addresses the pre-requisites to become an ethical hacker and also the **scope and limitations of ethical hacking**
- Discusses importance of **information security management** and Defense-in-Depth

- Discusses about information **security policies**, procedures, and awareness, and also physical security and controls
- Briefs various phases of **incident management process**
- Addresses the **vulnerability research** and **penetration testing process**
- Discusses various **information security acts and laws**

How to Teach this Module?

- Discuss various elements of information security
- Discuss various information security threats
- Explain the process of ethical hacking
- Discuss necessity, scope and limitations of ethical hacking
- Explain the importance of information security management
- Explain the process of incident management
- Explain the vulnerability research and penetration testing process for discovering security and design flaws
- Discuss various information security acts and laws

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wEr FrEE t0 FIY
HaCkRhInO-TeaM !

Exercise

This module does not contain any hands-on exercise.

Module 02: Footprinting and Reconnaissance

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wEr FrEE t0 FIY
HaCkRhInO-TeaM !

What is Covered in Module 02?

C|EH Certified Ethical Hacker

- Discusses **footprinting terminologies** and **threats**
- Briefs on the **footprinting methodologies** such as Internet footprinting, competitive intelligence gathering, network footprinting, etc.
- Provides an assessment of various **footprinting tools** used to collect information regarding a system or network

- Discusses various **footprinting countermeasures** to defend against footprinting attacks
- Describes various **penetration testing steps** involved in footprinting

How to Teach this Module?

C|EH Certified Ethical Hacker

Discuss various footprinting terminologies

Discuss various footprinting threats

Explain various footprinting methodologies such as WHOIS footprinting, DNS footprinting, E-mail footprinting, etc.

Discuss the penetration testing process

Discuss various footprinting countermeasures

Show various footprinting tools used to footprint a system/network

Exercise

Demonstrate the following labs:

- **Lab 01**: Open Source Information Gathering using Windows Command Line Utilities (Self Study)
- **Lab 02**: Gathering Personal Information using Online People Search Services (Self Study)
- **Lab 03**: Collecting Information about a Target Website Using Firebug
- **Lab 04**: Automating Information Gathering Using Web Data Extractor
- **Lab 05**: Mirroring Website Using HTTrack Web Site Copier
- **Lab 06**: Collecting Information about a Target by Tracing Emails
- **Lab 07**: Gathering IP and Domain Name Information Using Whois Lookup (Self Study)
- **Lab 08**: Advanced Network Route Tracing using Path Analyzer Pro
- **Lab 09**: Footprinting a Target Using Maltego
- **Lab 10**: Performing Automated Network Reconnaissance Using Recon-ng
- **Lab 11**: Using Open-source Reconnaissance Tool Recon-ng to Gather Personnel Information
- **Lab 12**: Collecting Information from Social Networking Sites Using Recon-ng Pushpin
- **Lab 13**: Automated Fingerprinting of an Organization Using FOCA
- **Lab 14**: Identifying Vulnerabilities and Information Disclosures in Search Engines Using SearchDiggity (Self Study)

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wEr FrEE t0 FIY
HaCkRhInO-TeaM !

Module 03: Scanning Networks

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wEr FrEE t0 FIY
HaCkRhInO-TeaM !

What is Covered in Module 03?

CEH Certified Ethical Hacker

The module briefs on **CEH scanning methodology** used to identify the vulnerabilities in a network that includes:

- Checking for live systems and ports
- Identifying services
- Banner grabbing/OS fingerprinting
- Scanning for vulnerabilities
- Drawing network diagrams of the vulnerable hosts
- Preparing proxies and anonymizers

- Discusses various **IP spoofing detection techniques**
- Discusses various **penetration testing steps** used to scan the network

How to Teach this Module?

1. Discuss various types of scanning
2. Explain CEH scanning methodology
3. Illustrate various scanning techniques such as SYN scan, FIN scan, IDLE scan, etc.
4. Explain how to defend against various scanning techniques
5. Discuss vulnerability scanning and network vulnerability scanners
6. Explain how to use proxies for an attack
7. Discuss various types of anonymizers
8. Discuss the penetration testing process

Exercise

C|EH Certified Ethical Hacker

Demonstrate the following labs:

- **Lab 01**: TCP and UDP Packet Crafting Techniques using HPING3
- **Lab 02**: Scanning the Network Using the Colasoft Packet Builder (Self Study)
- **Lab 03**: Basic Network Troubleshooting Using the MegaPing (Self Study)
- **Lab 04**: Understanding Network Scanning Using Nmap
- **Lab 05**: Exploring Various Network Scanning Techniques
- **Lab 06**: Scanning a Network Using the NetScan Tools Pro
- **Lab 07**: Avoiding Scanning Detection using Multiple Decoy IP Addresses
- **Lab 08**: Vulnerability Analysis Using the Nessus
- **Lab 09**: Scanning for Network Vulnerabilities Using the GFI LanGuard 2014 (Self Study)
- **Lab 10**: Drawing Network Diagrams Using Network Topology Mapper
- **Lab 11**: Scanning Devices in a Network using The Dude (Self Study)
- **Lab 12**: Daisy Chaining using Proxy Workbench
- **Lab 13**: Anonymous Browsing using Proxy Switcher (Self Study)
- **Lab 14**: Anonymous Browsing using CyberGhost (Self Study)

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wEr FrEE t0 FIY
HaCkRhInO-TeaM !

Module 04: Enumeration

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wEr FrEE t0 FIY
HaCkRhInO-TeaM !

What is Covered in Module 04?

C|EH Certified Ethical Hacker

This module explains the **process of extracting** user names, machine names, network resources, shares, and services from a system

Describes the **techniques for enumeration** such as NetBIOS Enumeration, SNMP enumeration, LDAP enumeration, NTP enumeration, SMTP enumeration, and DNS enumeration

Assesses various **penetration testing steps** used to extract the data from a system

Lists the enumeration tools that can be used to **extract the data**

How to Teach this Module?

CEH Certified Ethical Hacker

- Discuss the concept of enumeration
- Explain the enumeration process for various protocols such as SNMP, LDAP, NTP, SMTP and DNS
- Illustrate various tools to enumerate SNMP, LDAP, NTP, SMTP and DNS
- Explain how to defend against various enumerations
- Discuss the penetration testing process

Exercise

Demonstrate the following labs:

- **Lab 01**: NetBIOS Enumeration Using Global Network Inventory
- **Lab 02**: Enumerating Network Resources Using Advanced IP Scanner (Self Study)
- **Lab 03**: Performing Network Enumeration Using SuperScan (Self Study)
- **Lab 04**: Enumerating Resources in a Local Machine Using Hyena (Self Study)
- **Lab 05**: Performing Network Enumeration Using NetBIOS Enumerator (Self Study)
- **Lab 06**: Enumerating a Network Using SoftPerfect Network Scanner (Self Study)
- **Lab 07**: Enumerating a Target Network using Nmap and Net Use
- **Lab 08**: Enumerating Services on a Target Machine
- **Lab 09**: SNMP Enumeration Using SNMPCHECK
- **Lab 10**: LDAP Enumeration Using Active Directory Explorer (ADExplorer)
- **Lab 11**: Performing Network Enumeration Using Various DNS Interrogation Tools

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wEr FrEE t0 FIY
HaCkRhInO-TeaM !

Module 05: System Hacking

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wEr FrEE t0 FIY
HaCkRhInO-TeaM !

What is Covered in Module 05?

- Describes the CEH system hacking process which is classified into three stages: **gaining access** (by cracking passwords and escalating privileges), **maintaining access** (executing applications and hiding files), and **clearing logs** (covering tracks)
- Explains the **hacking tools** (keyloggers, spywares, and rootkits) that aid the hacking process
- Discusses various **steganography techniques** for hiding a secret message
- Presents the **countermeasures** that can be applied at every stage to prevent an attack on the system
- Discusses various **penetration testing steps**

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wEr FrEE t0 FIY
HaCkRhInO-TeaM !

How to Teach this Module?

- Discuss information at hand before system hacking stage
- Discuss various password attacks
- Explain how passwords are stored in Windows SAM
- Discuss the concept of privilege escalation
- Discuss various techniques to create and maintain remote access to the system
- Discuss various keystroke loggers and spywares

- Explain how to defend against keyloggers and spywares
- Discuss various types of rootkits and explain how they work
- Explain how to create NTFS streams and how to defend against it
- Illustrate the working of steganography technique and discuss its various types
- Discuss various techniques to hide the evidence of compromise
- Discuss the penetration testing process

Exercise

Demonstrate the following labs:

- **Lab 01**: Dumping and Cracking SAM Hashes to Extract Plaintext Passwords
- **Lab 02**: Creating and Using the Rainbow Tables
- **Lab 03**: Auditing System Passwords Using L0phtCrack (Self Study)
- **Lab 04**: Exploiting Client Side Vulnerabilities and Establishing a VNC Session
- **Lab 05**: Escalating Privileges by Exploiting Client Side Vulnerabilities
- **Lab 06**: Exploiting freeSSHd Vulnerability and Gaining Access to a Target System
- **Lab 07**: Hacking Windows 8.1 using Metasploit and Post Exploitation Using Meterpreter
- **Lab 08**: System Monitoring Using RemoteExec (Self Study)
- **Lab 09**: User System Monitoring and Surveillance Using Spytech SpyAgent
- **Lab 10**: Web Activity Monitoring and Recording using Power Spy 2014 (Self Study)
- **Lab 11**: Hiding Files Using NTFS Streams
- **Lab 12**: Find Hidden Files Using ADS Spy
- **Lab 13**: Hiding Data Using Snow Steganography
- **Lab 14**: Image Steganography Using OpenStego
- **Lab 15**: Image Steganography Using Quick Stego (Self Study)
- **Lab 16**: Viewing, Enabling and Clearing the Audit Policies Using Auditpol

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wEr FrEE t0 FIY
HaCkRhInO-TeaM !

Module 06: Malware Threats

What is Covered in Module 06?

C|EH Certified Ethical Hacker

- Discusses various malware and **malware propagation techniques**
- Discusses **Trojans** and **viruses**, their types, and how they infect files/systems
- Lists some of the **latest Trojans** that are used to infect a system
- Discusses **worms** that can compromise a business or system's security

- Explains the **malware analysis process**
- Discusses various scanning processes used to **detect Trojans**
- Briefs on the various methods of **virus detection**
- Lists **anti-malware tools**
- Discusses various **penetration testing steps** used to protect the system or network from the Malware

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wEr FrEE t0 FIY
HaCkRhInO-TeaM !

How to Teach this Module?

- Explain **malware** and discuss various malware propagation techniques
- Explain **how to infect systems** using a Trojan
- Explain how attackers **deploy a Trojan**
- Discuss various **types of Trojans**
- Explain various **characteristics of a virus** and different stages of virus life
- Explain the **working of virus** and indications of virus attack

- Discuss various **types of viruses** and explain how they infect the system
- Discuss **computer worms**
- Discuss the **malware analysis procedure**
- Discuss famous **Trojans**, **viruses**, and **worms**
- Explain **how to detect Trojans** using various techniques
- Explain **how to defend** against Trojans, viruses, and worms
- Discuss the **malware penetration testing process**

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wEr FrEE t0 FIY
HaCkRhInO-TeaM !

Exercise

C|EH Certified Ethical Hacker

Demonstrate the following labs:

- Lab 01: Creating a HTTP Trojan and Remotely Controlling a Target Machine Using HTTP RAT (Self Study)
- Lab 02: Creating a Trojan Server Using the GUI Trojan MoSucker (Self Study)
- Lab 03: Gaining Control over a Victim machine Using njRAT
- Lab 04: Obfuscating a Trojan Using SwayzCryptor and Making it Undetectable from Various Anti-Virus Programs
- Lab 05: Creating a Trojan Server Using the ProRat Tool (Self Study)
- Lab 06: Creating a Trojan Server Using the Theef (Self Study)
- Lab 07: Attaining Remote Access Using Atelier Web Remote Commander (Self Study)
- Lab 08: Building a Botnet Infrastructure Using Umbra Loader
- Lab 09: Creating a Virus Using the JPS Virus Maker Tool
- Lab 10: Creating a Worm Using Ghost Eye Worm and maintaining a Persistent Connection Using njRAT
- Lab 11: Creating a Worm Using the Internet Worm Maker Thing
- Lab 12: Virus analysis using IDA Pro
- Lab 13: Virus analysis using Virus Total (Self Study)
- Lab 14: Virus Analysis Using OllyDbg (Self Study)
- Lab 15: Detecting Trojans
- Lab 16: Monitoring TCP/IP Connections Using the CurrPorts

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wEr FrEE t0 FIY
HaCkRhInO-TeaM !

Module 07: Sniffing

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wEr FrEE t0 FIY
HaCkRhInO-TeaM !

What is Covered in Module 07?

C|EH Certified Ethical Hacker

- Briefs about the basic concepts of sniffing network and various types of sniffing
- Delineates MAC flooding and how to defend against this attack
- Explains the working of DHCP and various DHCP attacks
- Defines ARP and describes the working of ARP spoofing in detail
- Lists various threats of ARP Poisoning and tools used to conduct this attack

- Assess diverse DNS poisoning techniques and explains how to secure against them
- Features versatile sniffing tools and explains how an attacker hacks a network using them
- Lists a number of countermeasures to defend against sniffing
- Discusses various penetration testing steps

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wEr FrEE t0 FIY
HaCkRhInO-TeaM !

How to Teach this Module?

1. Define the term sniffing and explain the types of sniffing
2. Describe MAC flooding and how to defend against this attack
3. Identify and explain various threats of ARP Poisoning and exhibit tools used to conduct this attack
4. Elaborate various DNS poisoning techniques and explain in detail how to secure against them
5. Demonstrate various sniffing tools and show how an attacker hacks a network using them
6. Explain sniffing prevention techniques and tools used to defend against sniffing
7. Discuss the penetration testing process

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wEr FrEE t0 FIY
HaCkRhInO-TeaM !

Exercise

C|EH Certified Ethical Hacker

Demonstrate the following labs:

- **Lab 01**: Sniffing Passwords using Wireshark
- **Lab 02**: Analyzing a Network Using the Capsa Network Analyzer (Self Study)
- **Lab 03**: Sniffing the Network Using the OmniPeek Network Analyzer (Self Study)
- **Lab 04**: Spoofing MAC Address Using SMAC
- **Lab 05**: Performing Man-in-the-Middle Attack using Cain & Abel
- **Lab 06**: Detecting Systems running in Promiscuous Mode in a Network using PromqryUI
- **Lab 07**: Detecting ARP Poisoning in a Switch Based Network
- **Lab 08**: Detecting ARP Attacks with XArp Tool (Self Study)

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wEr FrEE t0 FIY
HaCkRhInO-TeaM !

Module 08: Social Engineering

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wEr FrEE t0 FIY
HaCkRhInO-TeaM !

What is Covered in Module 08?

C|EH Certified Ethical Hacker

- Introduces social engineering and various **attack phases**
- Describes the **types of social engineering** with examples
- Tabulates common intrusion tactics and proposes **combat strategies** to prevent such attacks
- Explains in detail how **impersonation on social engineering sites** is carried out

- Briefs how attackers obtain and exploit **personally identifiable information** and authenticate themselves, in order to impersonate victim
- Quotes various social engineering and **identity theft countermeasures**
- Lists anti-phishing tools to detect phishing emails and websites
- Talks about social engineering penetration testing

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wEr FrEE t0 FIY
HaCkRhInO-TeaM !

How to Teach this Module?

- Explain what is social engineering and its phases
- Discuss the common targets of social engineering attack
- Illustrate common intrusion tactics and prevention strategies
- List the factors that make companies vulnerable to social engineering attacks
- Describe what is identity theft and how to steal identity?
- Discuss social engineering and identity theft countermeasures
- Discuss social engineering pen testing

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wEr FrEE t0 FIY
HaCkRhInO-TeaM !

Exercise

C|EH Certified Ethical Hacker

Demonstrate the following labs:

- **Lab 01**: Detecting Phishing Using Netcraft
- **Lab 02**: Detecting Phishing Using PhishTank (Self Study)
- **Lab 03**: Sniffing Facebook Credentials using Social Engineering Toolkit (SET)
- **Lab 04**: Creating a Malicious Payload Using SET and Exploiting a Windows Machine

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wEr FrEE t0 FIY
HaCkRhInO-TeaM !

Module 09: Denial-of-Service

What is Covered in Module 09?

C|EH Certified Ethical Hacker

This module explains **DoS/DDoS attacks**, the classification of DoS/DDoS attacks, and various attack techniques

This module discusses **Botnets**, the types of bots, and how they infect the system

Explains **countermeasures** to prevent DoS/DDoS attacks and pen testing steps

The module demonstrates various **tools to perform DoS and DDoS** attacks

How to Teach this Module?

C|EH Certified Ethical Hacker

Discuss the various DoS **Penetration Testing steps**

Discuss the various **countermeasures** to defend DoS attack

Showcase few specific **tools and techniques** used to demonstrate DoS attacks

Discuss the DoS Attack **Methodology**

Explain various **DoS Concepts** and attack techniques

Describe some of the common **DoS/DDoS attack techniques**

Describe **Bots** and **Botnets** with the use of examples

Explain how **malicious code propagates**?

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wEr FrEE t0 FIY
HaCkRhInO-TeaM !

Exercise

C|EH Certified Ethical Hacker

Demonstrate the following labs:

- **Lab 01**: SYN Flooding a Target Host Using Metasploit
- **Lab 02**: SYN Flooding a Target Host Using hping3 (Self Study)
- **Lab 03**: HTTP Flooding using DoSHTTP
- **Lab 04**: Implementing DoS Attack on a Router using Slowloris Script
- **Lab 05**: Performing Distributed Denial of Service Attack Using HOIC
- **Lab 06**: Detecting and Analyzing DoS Attack Traffic Using KFSensor and Wireshark

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wEr FrEE t0 FIY
HaCkRhInO-TeaM !

Module 10: Session Hijacking

What is Covered in Module 10?

C|EH Certified Ethical Hacker

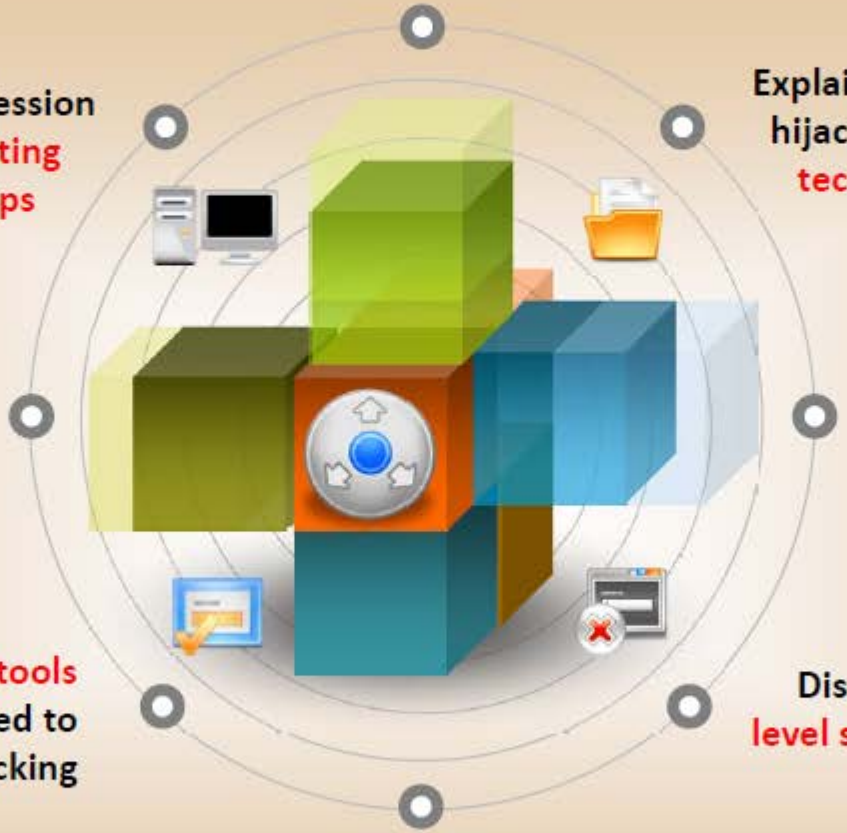
1. This module explains session hijacking concepts

2. Demonstrates various key session hijacking techniques and tools

3. Explains countermeasures to prevent session hijacking attacks

4. Discusses the various penetration testing steps involved in session hijacking

How to Teach this Module?



Discuss the various session hijacking penetration testing steps

Explain various session hijacking concepts and attack techniques

Discuss the various countermeasures to defend against session hijacking attacks

Explain the difference Spoofing vs. Hijacking

Showcase few specific tools and techniques used to perform session hijacking

Discuss various application level session hijacking attacks

Discuss various network level session hijacking attack

Exercise

C|EH Certified Ethical Hacker

Demonstrate the following labs:

- **Lab 01**: Session Hijacking Using the Zed Attack Proxy (ZAP)
- **Lab 02**: Hijacking a User Session Using Firebug
- **Lab 03**: Hijacking HTTPS Traffic in a Network Using sslstrip
- **Lab 04**: Performing a MiTM Attack and Hijacking an Established Session Using Websploit

Module 11: Hacking Webservers

What is Covered in Module 11?

This module discusses various reasons why web servers are compromised

Explains open source webserver and IIS architecture

Demonstrates various key webserver attack techniques and tools

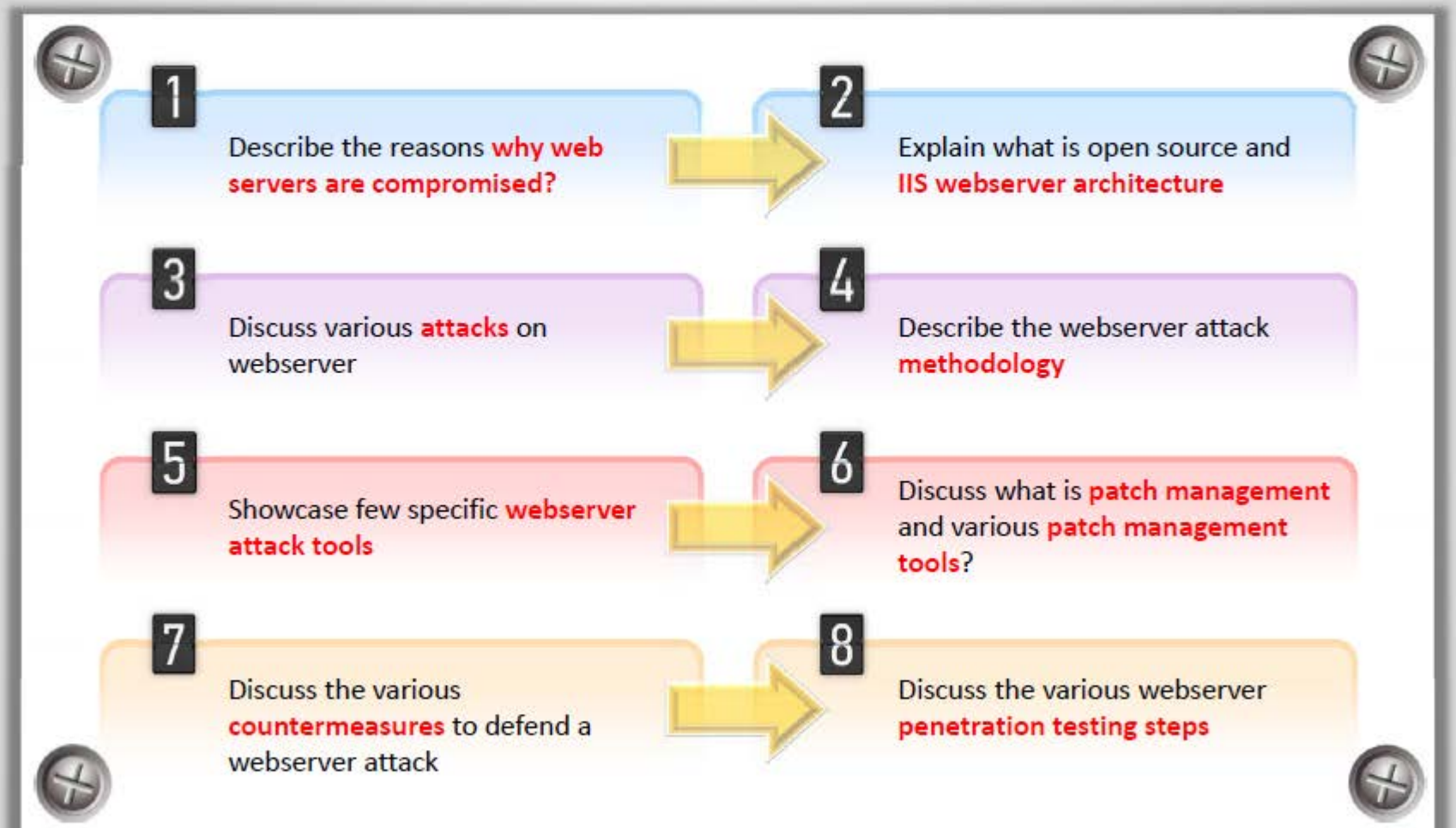
Explains countermeasures to prevent webserver attacks

Explains what is patch management and associated concepts

Discusses the various penetration testing steps involved in Webserver Pen Testing

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wEr FrEE t0 FIY
HaCkRhInO-TeaM !

How to Teach this Module?



HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wEr FrEE t0 FIY
HaCkRhInO-TeaM !

Exercise

C|EH Certified Ethical Hacker

Demonstrate the following labs:

- **Lab 01**: Performing Web Server Reconnaissance using Skipfish
- **Lab 02**: Footprinting Webserver Using the httprecon Tool (Self Study)
- **Lab 03**: Footprinting a Webserver Using ID Serve (Self Study)
- **Lab 04**: Exploiting Java Vulnerability using Metasploit Framework
- **Lab 05**: Performing ShellShock Exploitation on a Web Server and Gaining Unrestricted Access to the Server
- **Lab 06**: Cracking FTP Credentials Using Dictionary Attack

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wEr FrEE t0 FIY
HaCkRhInO-TeaM !

Module 12: Hacking Web Applications

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wEr FrEE t0 FIY
HaCkRhInO-TeaM !

What is Covered in Module 12?

C|EH Certified Ethical Hacker

This module gives an introduction to **web applications** and their components

Describes **web application architecture** and demonstrates how web applications work?

Lists and explain various **web application threats and attacks**

Discusses the various **penetration testing steps** involved in web application pen testing

Demonstrates various Key **web application hacking** and security tools

Explains **web app hacking** methodology

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wEr FrEE t0 FIY
HaCkRhInO-TeaM !

How to Teach this Module?

C|EH Certified Ethical Hacker

1. Explain how web applications work?
2. Give a brief introduction about what are Web 2.0 applications
3. Explain what is a vulnerability stack and different web attack vectors
4. List and explain the various web application threats and examples
5. Describe the web app hacking methodology
6. Discuss the various countermeasures to defend a web application attack
7. Discuss the various web application penetration testing steps

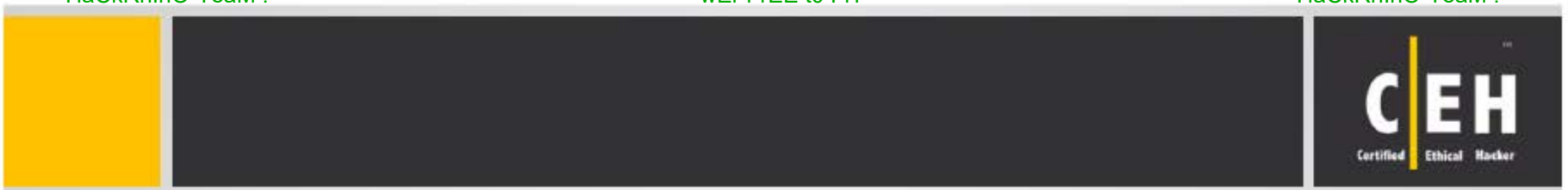
HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wEr FrEE t0 FIY
HaCkRhInO-TeaM !

Exercise

C|EH Certified Ethical Hacker

Demonstrate the following labs:

- **Lab 01**: Exploiting Parameter Tampering and XSS Vulnerabilities in Web Applications
- **Lab 02**: Using Stored XSS Attack to Hijack an Authenticated User Session
- **Lab 03**: Enumerating and Hacking a Web Application Using WPScan and Metasploit
- **Lab 04**: Exploiting WordPress Plugin Vulnerabilities using Metasploit
- **Lab 05**: Exploiting Remote Command Execution Vulnerability to Compromise a Target Web Server
- **Lab 06**: Auditing Web Application Framework Using W3AF
- **Lab 07**: Website Vulnerability Scanning Using Acunetix WVS (Self Study)



Module 13: SQL Injection

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wEr FrEE t0 FIY
HaCkRhInO-TeaM !

What is Covered in Module 13?

C|EH Certified Ethical Hacker

- This module gives an introduction to SQL Injection and **threats from SQL injection attacks**
- Explains SQL injection **detection mechanisms** and the **types of SQL injection attacks**
- Explains **SQL injection methodology**
- Demonstrates various key **SQL injection tools** and **detection tools**
- Discusses how to **defend** against SQL injection attacks

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wEr FrEE t0 FIY
HaCkRhInO-TeaM !

How to Teach this Module?

1. Give a brief introduction to SQL injection

2. Give various example of a Web app vulnerable to SQL injection

3. List and explain the various forms of SQL injection attack

4. Discuss SQL injection methodology

5. Demonstrate various key SQL injection and detection tools

6. Discuss the various countermeasures to defend SQL injection attack

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wEr FrEE t0 FIY
HaCkRhInO-TeaM !

Exercise

Demonstrate the following labs:

- **Lab 01**: SQL Injection Attacks on MS SQL Database
- **Lab 02**: Performing Blind SQL Injection on DVWA Application
- **Lab 03**: Testing for SQL Injection Using IBM Security AppScan Tool (Self Study)
- **Lab 04**: Testing for SQL Injection Using WebCruiser Tool (Self Study)
- **Lab 05**: Scanning Web Applications Using N-Stalker Tool

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wEr FrEE t0 FIY
HaCkRhInO-TeaM !

Module 14: Hacking Wireless Networks

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wEr FrEE t0 FIY
HaCkRhInO-TeaM !

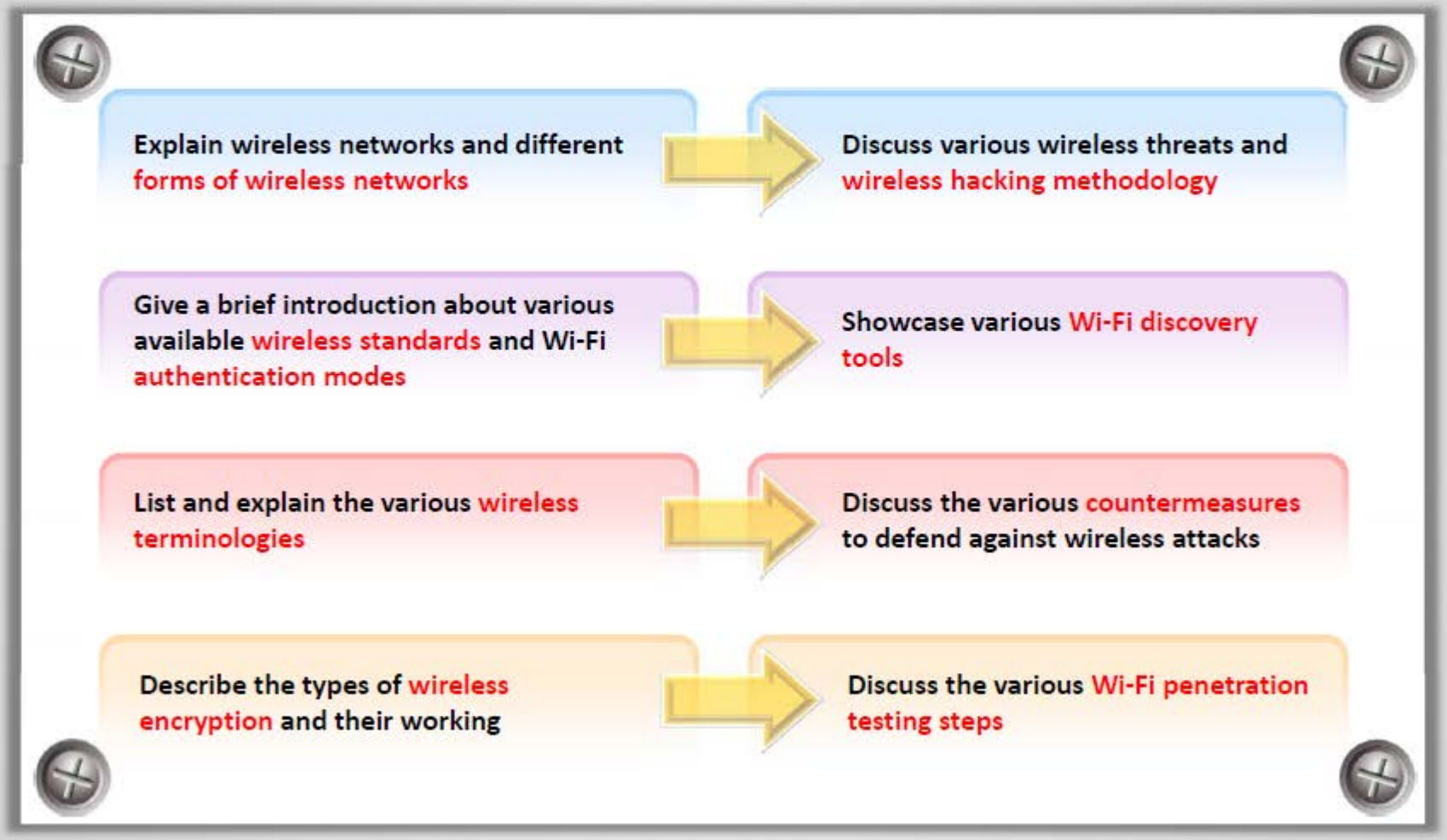
What is Covered in Module 14?

C|EH Certified Ethical Hacker

1	The module gives an introduction to wireless networks and explores their advantages and disadvantages	Lists and explains various wireless threats	6
2	Explains the types of wireless networks	Describes wireless hacking methodology	7
3	Discusses the various wireless standards and Wi-Fi authentication modes	Demonstrates various key Wi-Fi discovery tools	8
4	Lists the various wireless terminologies	Discusses how to defend against wireless attacks	9
5	Discusses the types of wireless encryption and their working	Discusses the various Wi-Fi penetration testing steps	10

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wEr FrEE t0 FIY
HaCkRhInO-TeaM !

How to Teach This Module?



HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wEr FrEE t0 FIY
HaCkRhInO-TeaM !

Exercise

C|EH Certified Ethical Hacker

Demonstrate the following labs:

- **Lab 01**: WiFi Packet Sniffing Using AirPcap with Wireshark
- **Lab 02**: Sniffing the Network Using the OmniPeek Network Analyzer (Self Study)
- **Lab 03**: Cracking a WEP Network with Aircrack-ng for Windows

Note: In case AirPcap adapter is not available, you can use a normal Wi-Fi adapter to demonstrate these labs.

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wEr FrEE t0 FIY
HaCkRhInO-TeaM !

Module 15: Hacking Mobile Platforms

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wEr FrEE t0 FIY
HaCkRhInO-TeaM !

What is Covered in Module 15?

This module discusses mobile attack vectors in detail and explores app sandboxing issues

Discusses Android OS architecture briefly and demonstrates hacking android OS using various tools

Gives a brief knowledge on jailbreaking iOS, its types, techniques and tools required for jailbreaking

Describes Windows Phone 8 architecture and explains guidelines for securing windows OS devices

Explains Blackberry Enterprise solution architecture, lists various types of exploits and guidelines for securing blackberry devices

Provides brief knowledge on mobile security guidelines

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wEr FrEE t0 FIY
HaCkRhInO-TeaM !

How to Teach This Module?

Explain various terminologies and discuss mobile attack vector

Describe Android OS architecture and demonstrate android rooting using various tools

Showcase few tools and techniques to demonstrate iOS jailbreaking

Explain Windows Phone 8 architecture and discuss secure boot process along with the guidelines for securing windows OS devices

Elaborate Blackberry enterprise solution architecture and explain various attacks and exploits

Explain various mobile security guidelines and discuss the various mobile penetration testing steps

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wEr FrEE t0 FIY
HaCkRhInO-TeaM !

Exercise

C|EH Certified Ethical Hacker

Demonstrate the following labs:

- **Lab 01**: Creating Binary Payloads using Kali Linux to Hack Android
- **Lab 02**: Harvesting Users' Credentials Using Social Engineering Toolkit
- **Lab 03**: Using Mobile Platform to Enforce a DoS Attack on a Victim Machine
- **Lab 04**: Securing Android Device from Malicious Applications

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wEr FrEE t0 FIY
HaCkRhInO-TeaM !

Module 16: Evading IDS, Firewalls, and Honeypots

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wEr FrEE t0 FIY
HaCkRhInO-TeaM !

What is Covered in Module 16?

C|EH Certified Ethical Hacker

- This module gives an introduction IDS, firewall and honeypot concepts
- Explains the intrusion detection systems (IDS) and their placement
- Lists the various general indications of intrusions
- Describes various evasion attacks
- Explains what is firewall, architecture, and its types
- Discusses the concepts of honeypots and describes how to setup a honeypot
- Demonstrates Snort and its rules
- Lists various honeypot detecting and firewall evasion tools
- Discusses the countermeasures
- Discusses the various steps in firewall/IDS penetration testing steps

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wEr FrEE t0 FIY
HaCkRhInO-TeaM !

How to Teach This Module?



- Describe briefly intrusion detection Systems (IDS) and their placement
- List and explain the various indications of intrusions and evasion attacks
- Explain what is firewall, architecture, and its types
- Discuss the concepts of honeypots and describes how to setup a honeypot
- Demonstrate Snort and its rules and list IDS, firewall and honeypot solutions
- Discuss various techniques to evade IDS and firewall
- Explain how to detect honeypots
- Discuss the countermeasures
- Assess the various steps in firewall/IDS penetration testing steps

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wEr FrEE t0 FIY
HaCkRhInO-TeaM !

Exercise

C|EH Certified Ethical Hacker

Demonstrate the following labs:

- **Lab 01**: Detecting Intrusions using Snort
- **Lab 02**: Detecting Malicious Traffic on Network using HoneyBot
- **Lab 03**: Detecting Intruders and Worms using KFSensor Honeypot IDS (Self Study)
- **Lab 04**: Bypassing Windows Firewall Using Nmap Evasion Techniques
- **Lab 05**: Bypassing Firewall Rules Using HTTP/FTP Tunneling
- **Lab 06**: Bypassing Windows Firewall and Maintaining a Persistent Connection with a Victim

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wEr FrEE t0 FIY
HaCkRhInO-TeaM !

Module 17: Cloud Computing

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wEr FrEE t0 FIY
HaCkRhInO-TeaM !

What is Covered in Module 17?

C|EH Certified Ethical Hacker

- Briefs about the basic concepts of cloud computing and various types of cloud computing services
- Explains the importance of virtualization in cloud computing
- Lists various threats of cloud computing
- Discusses various cloud computing attacks

- Briefs about various cloud computing security considerations
- Discusses best practices for securing cloud
- Discusses various cloud security tools
- Discusses various cloud penetration testing steps

How to Teach this Module?

1. Define the term cloud computing and explain the types of cloud computing services
2. Explain why virtualization is important in building cloud environment
3. Discuss various threats to cloud computing
4. Explain various cloud computing attacks
5. Discuss best practices for securing cloud
6. Demonstrate various cloud security tools
7. Discuss the penetration testing process

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wEr FrEE t0 FIY
HaCkRhInO-TeaM !

Exercise

C|EH Certified Ethical Hacker

Demonstrate the following labs:

- **Lab 01**: Building a Cloud Using ownCloud and WampServer
- **Lab 02**: Transferring Cloud Data Over Secure Channel
- **Lab 03**: Harvesting Cloud Credentials by Exploiting Java Vulnerability
- **Lab 04**: Performing Cloud Vulnerability Assessment Using Mobile Based Security Scanner zANTI

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wEr FrEE t0 FIY
HaCkRhInO-TeaM !

Module 18: Cryptography

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wEr FrEE t0 FIY
HaCkRhInO-TeaM !

What is Covered in Module 18?

C|EH Certified Ethical Hacker

- This module gives an introduction to **cryptography concepts**
- Lists the types of cryptography and their **working process**
- Discusses **ciphers** and its types
- Explains about Advanced Encryption Standard (**AES**) and Data Encryption Standard (**DES**)
- Discusses Rivest Shamir Adleman (**RSA**) with an example

- Features versatile **cryptography tools**
- Explains Public Key Infrastructure (**PKI**) and its components
- Discusses email encryption, disk encryption, and **cryptography attacks**
- Explains how to **defend** against cryptography attacks

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wEr FrEE t0 FIY
HaCkRhInO-TeaM !

How to Teach this Module?

1. Explain cryptography concepts
2. Discuss the types of cryptography and their function
3. Explain the working methodology of ciphers
4. Explain the Advanced Encryption Standard (AES) and Data Encryption Standard (DES)
5. Examine Rivert Shamir Adleman with an example
6. Demonstrate the function of MD5 Hash Calculators
7. Discuss Public Key Infrastructure (PKI) and its components

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wEr FrEE t0 FIY
HaCkRhInO-TeaM !

Exercise

C|EH Certified Ethical Hacker

Demonstrate the following labs:

- Lab 01: Calculating MD5 Hashes and Verifying File Integrity Using Quick Checksum Verifier
- Lab 02: Calculating One-way Hashes Using HashCalc (Self Study)
- Lab 03: Calculating MD5 Hashes Using MD5 Calculator (Self Study)
- Lab 04: Understanding File and Text Encryption Using CryptoForge
- Lab 05: Basic Data Encryption Using Advanced Encryption Package (Self Study)
- Lab 06: Encrypting and Decrypting the Data Using BCTextEncoder (Self Study)
- Lab 07: Exploiting OpenSSL Heartbleed Vulnerability on a HTTPS website
- Lab 08: Creating and Using Self-Signed Certificates
- Lab 09: Basic Disk Encryption Using VeraCrypt
- Lab 10: Basic Data Encrypting Using Rohos Disk Encryption (Self Study)
- Lab 11: Basic Data Encryption Using CrypTool

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wEr FrEE t0 FIY
HaCkRhInO-TeaM !