

TAKEDØWNCON
www.takedowncon.com

TAKEDØWNCON is a hacking conference that was conceived by our members! EC-Council has been flooded with requests to take our world-class courses on the road! We have answered the call and created TakeDownCon! This conference will be focused on the learner and will feature several Certification & Certificate Training courses for Advanced Practitioners!

TAKEDØWNCON will host EC-Council's sought after Hacking, Forensics and Pen Test courses, Certified Wireless Security Professional, and several highly technical and advanced workshops which will cover current and important security topics such as advanced penetration testing, cryptography, network defense, application security and mobile forensics.

At **TAKEDØWNCON** the learning doesn't stop when the training ends! We have lined up a list of sought after industry practitioners and subject matter experts that will present relevant and implementable topics!

*For more information, about **TAKEDØWNCON** please visit www.takedowncon.com*



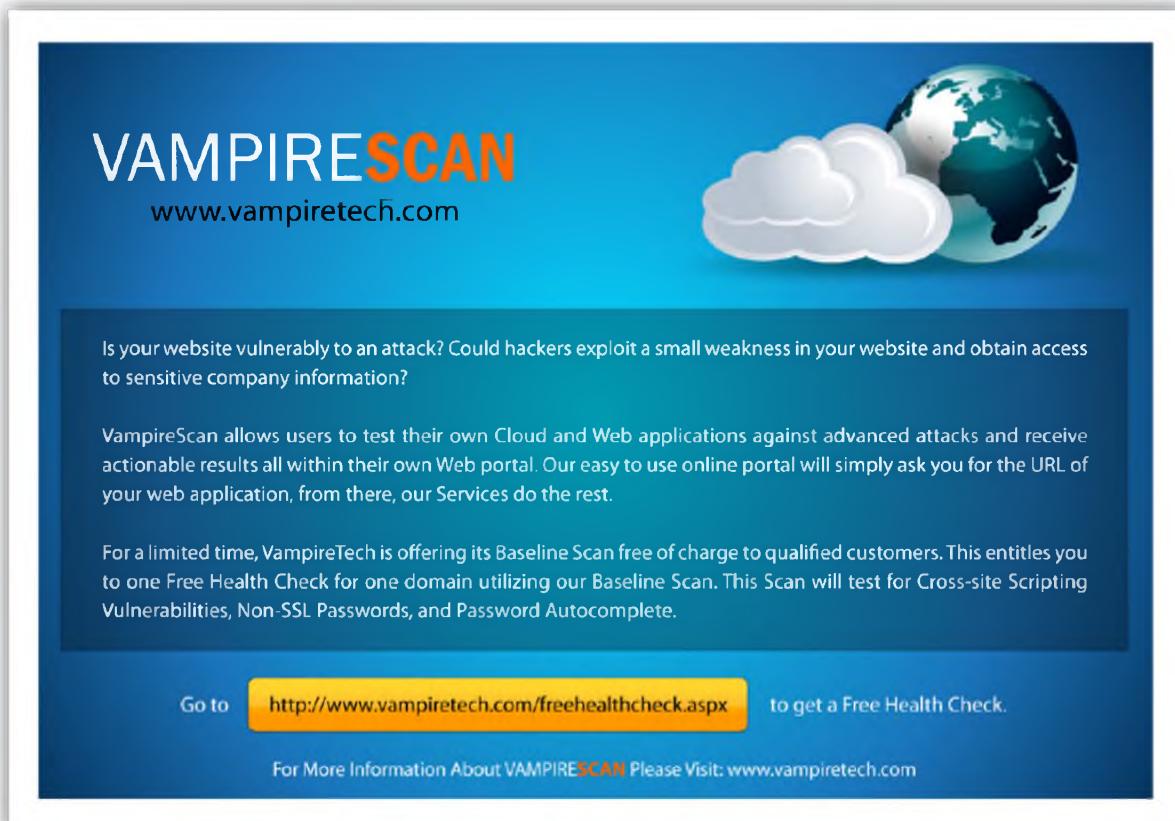
Hacker | Halted
www.hackerhalted.com

Since 2004 EC-Council has hosted 20 Hacker Halted events across four continents and in cities such as Myrtle Beach, Miami, Dubai, Singapore, Hong Kong, Mexico City, Tokyo, Kuala Lumpur, Guangzhou, Taipei and Cairo.

Hacker Halted North America will be held in Miami for the 3rd year in a row and based on past history is sure to boast an amazing turnout of Information Security Professionals!

Hacker Halted is more than just a conference event; practitioners travel from all over the world to attend our world-class training, gain practical knowledge from our expert presenters and get a preview of the latest technologies and Information Security tools which will be showcased by our exhibitors and partners.

*For more information, about **Hacker Halted** please visit www.hackerhalted.com*



The banner features the logo "VAMPIRESCAN" in large white and orange letters, with the website "www.vampiretech.com" below it. To the right is a graphic of a globe partially obscured by a white cloud. The background is a gradient from dark blue at the top to light blue at the bottom.

Is your website vulnerably to an attack? Could hackers exploit a small weakness in your website and obtain access to sensitive company information?

VampireScan allows users to test their own Cloud and Web applications against advanced attacks and receive actionable results all within their own Web portal. Our easy to use online portal will simply ask you for the URL of your web application, from there, our Services do the rest.

For a limited time, VampireTech is offering its Baseline Scan free of charge to qualified customers. This entitles you to one Free Health Check for one domain utilizing our Baseline Scan. This Scan will test for Cross-site Scripting Vulnerabilities, Non-SSL Passwords, and Password Autocomplete.

Go to <http://www.vampiretech.com/freehealthcheck.aspx> to get a Free Health Check.

For More Information About VAMPIRESCAN Please Visit: www.vampiretech.com



A photograph of several men in business attire seated at a conference table with microphones, suggesting a panel discussion or summit. A black arrow-shaped callout points from the right side of the image towards the text.

Global CISO Executive Summit

Be on the forefront of a new global initiative where today's world-class leaders in information security will gather to navigate through international waters. Join these leaders as they follow the wind of change that is sweeping through the IS community motivating today's information guardians to develop a new way of thinking to ensure success in protecting their respective organizations.

The goal of EC-Council's Global CISO Forum is to create an open platform for top information security executives to discuss their successes, failures, obstacles, and challenges. The open conversation will lead to the creation of actionable items that can be discussed and applied to the organization.

For More Information About CISO Executive Summit Please Visit: www.eccouncil.org/resources/ciso-executive-summit.aspx

How to Download My CEHv8 E-Courseware and Additional Lab Manuals?

Please follow the steps below to download your CEHv8 e-courseware and additional lab manual.

Step 1:

Visit: <https://academia.eccouncil.org>. If you have an account already, skip to Step 4.

Step 2:

Click Register and fill out the registration form.

Step 3:

Using the email you provided in step 2, follow the instructions in the auto-generated email to activate your Academia Portal account.

Step 4:

Login using your Username and Password.

Step 5:

Once successfully logged in, expand the **About Academia** navigation menu and select **Access Code**.

Step 6:

Enter the access code provided to you to redeem access to the CEH V8 e-Courseware and Lab Manuals.

Access Code: XXXXXXXXXXXXXXXXXX

Step 8:

Once redeemed, expand the **Courses** menu and select **iLearn – PDF Courseware** – The resulting page will list your CEH v8 e-Courseware and Lab Manuals.

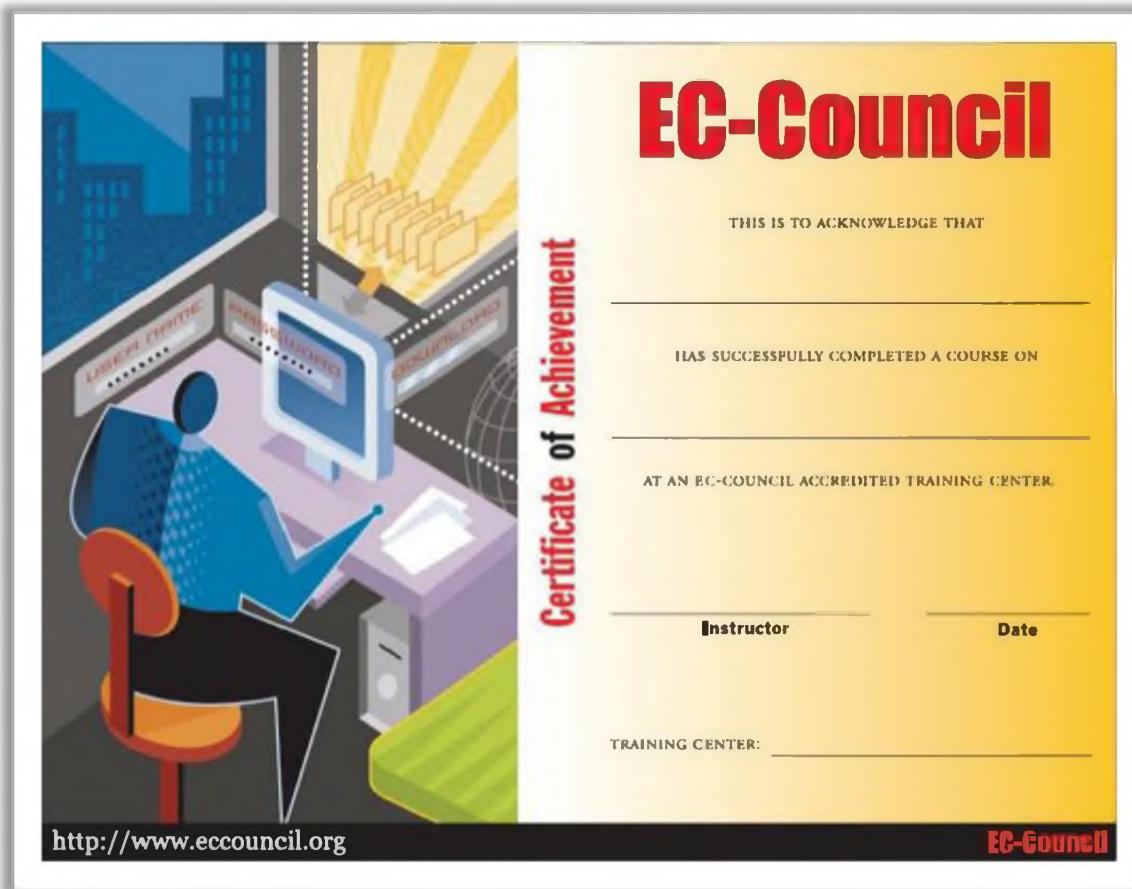
Support:

E-mail support is available from academia@eccouncil.org.

System Requirements:

Visit <https://academia.eccouncil.org/AboutAcademia/WhatisiLearn.aspx> to view the system requirements.

Download Class Certificate of Attendance



Please follow the below stated steps to download digital copy (PDF format) of your class certificate of attendance.

Step 1: Wait until the class is over (the last of the class).

Step 2: Visit <http://www.eccouncil.org/eval>.

Step 3: Complete the course evaluation form (please complete all the fields in the form – correct e-mail address is required).

Step 4: Evaluation code is required to submit the form. See the attached code.

Step 5: Submit the form.

Step 6: A web link will be sent to you to download your PDF copy of the certificate.

Course Evaluation Code: **CEH-*******

Ethical Hacking and Countermeasures

Version 8

EC-Council

Copyright © 2013 by EC-Council. All rights reserved. Except as permitted under the Copyright Act of 1976, no part of this publication may be reproduced or distributed in any form or by any means, or stored in a database or retrieval system, without the prior written permission of the publisher, with the exception that the program listings may be entered, stored, and executed in a computer system, but they may not be reproduced for publication.

Information has been obtained by EC-Council from sources believed to be reliable. EC-Council uses reasonable endeavors to ensure that the content is current and accurate, however, because of the possibility of human or mechanical error we do not guarantee the accuracy, adequacy, or completeness of any information and are not responsible for any errors or omissions or the accuracy of the results obtained from use of such information.

The courseware is a result of extensive research and contributions from subject matter experts from the field from all over the world. Due credits for all such contributions and references are given in the courseware in the research endnotes. We are committed towards protecting intellectual property. If you are a copyright owner (an exclusive licensee or their agent), and if you believe that any part of the courseware constitutes an infringement of copyright, or a breach of an agreed licence or contract, you may notify us at legal@eccouncil.org. In the event of a justified complaint, EC-Council will remove the material in question and make necessary rectifications.

The courseware may contain references to other information resources and security solutions, but such references should not be considered as an endorsement of or recommendation by EC-Council.

Readers are encouraged to report errors, omissions and inaccuracies to EC-Council at legal@eccouncil.org.

If you have any issues, please contact support@eccouncil.org.

Foreword

Since you are reading this CEHv8 courseware, you most likely realize the importance of information systems security. However, we would like to put forth our motive behind compiling a resource such as this one and what you can gain from this course.

You might find yourself asking what sets this course apart from the others out there. The truth is that no single courseware can address all the issues of information security in a detailed manner. Moreover, the rate at which exploits, tools, and methods are being discovered by the security community makes it difficult for one program to cover all the necessary facets of information security. This doesn't mean that this course is inadequate in any way as we have worked to cover all major domains in such a manner that the reader will be able to appreciate the way security has evolved over time as well as gain insight into the fundamental workings relevant to each domain. It is a blend of academic and practical wisdom supplemented with tools that the reader can readily access in order to obtain a hands-on experience.

The emphasis throughout the courseware is on gaining practical know-how, which explains the stress on free and accessible tools. You will read about some of the most widespread attacks seen, the popular tools used by attackers, and how attacks have been carried out using ordinary resources.

You may also want to know what to expect once you have completed the course. This courseware is a resource material. Any penetration tester can tell you that there is no one straight methodology or sequence of steps that you can follow while auditing a client site. There is no one template that will meet all your needs. Your testing strategy will vary with the client, the basic information about the system or situation, and the resources at your disposal. However, for each stage you choose – be it enumeration, firewall, penetration of other domains - you will find something in this courseware that you can definitely use.

Finally this is not the end! This courseware is to be considered a constant work-in-progress because we will be adding value to this courseware over time. You may find some aspects extremely detailed, while others may have less detail. We are constantly asking ourselves if the content helps explain the core point of the lesson, and we constantly calibrate our material with that in mind. We would love to hear your viewpoints and suggestions so please send us your feedback to help in our quest to constantly improve our courseware.

This page is intentionally left blank.

Table of Contents

Module Number	Module Name	Page No.
00	Student Introduction	I
01	Introduction to Ethical Hacking	01
02	Footprinting and Reconnaissance	91
03	Scanning Networks	262
04	Enumeration	434
05	System Hacking	517
06	Trojans and Backdoors	827
07	Viruses and Worms	1006
08	Sniffing	1112
09	Social Engineering	1292
10	Denial of Service	1402
11	Session Hijacking	1503
12	Hacking Webservers	1600
13	Hacking Web Applications	1723
14	SQL Injection	1986
15	Hacking Wireless Networks	2134
16	Hacking Mobile Platforms	2392
17	Evading IDS, Firewalls, and Honeypots	2549
18	Buffer Overflow	2691
19	Cryptography	2782
20	Penetration Testing	2872
	References	2976

This page is intentionally left blank.



Ethical Hacking and Countermeasures

Module 00: Welcome to Certified Ethical Hacker Class

Exam 312-50

Introduction

CEH
Certified Ethical Hacker

- 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

CEH
Certified Ethical Hacker



Identity Card



Student Courseware



Lab Manual/
Workbook



Compact Disc



Course
Evaluation



Reference
Materials

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

CEHv8 Course Outline

The diagram shows a 2x5 grid of course modules. The first column contains modules 1 through 5. The second column contains modules 6 through 10. Modules 1, 2, 3, 4, and 5 are in grey boxes. Modules 6, 7, 8, 9, and 10 are in white boxes with black outlines. The CEH logo is in the top right corner.

1	Introduction to Ethical Hacking	6	Trojans and Backdoors
2	Footprinting and Reconnaissance	7	Viruses and Worms
3	Scanning Networks	8	Sniffing
4	Enumeration	9	Social Engineering
5	System Hacking	10	Denial-of-Service

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

CEHv8 Course Outline

The diagram shows a 2x10 grid of course modules. The first column contains modules 11 through 15. The second column contains modules 16 through 20. Modules 11, 12, 13, 14, and 15 are in grey boxes. Modules 16, 17, 18, 19, and 20 are in white boxes with black outlines. The CEH logo is in the top right corner.

11	Session Hijacking	16	Hacking Mobile Platforms
12	Hacking Webservers	17	Evading IDS, Firewalls and Honeypots
13	Hacking Web Applications	18	Buffer Overflows
14	SQL Injection	19	Cryptography
15	Hacking Wireless Networks	20	Penetration Testing

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

EC-Council Certification Program

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

Certified Secure Computer User (CSCU)	EC-Council Disaster Recovery Professional (EDRP)
Certified e-Business Professional	EC-Council Certified Security Analyst (ECSA)
EC-Council Certified Security Specialist (ECSS)	EC-Council Certified Secure Programmer (ECSP)
EC-Council Network Security Administrator (ENSA)	Certified Secure Application Developer (CSAD)
Certified Ethical Hacker (CEH) <small>You are here</small>	Licensed Penetration Tester (LPT)
Computer Hacking Forensic Investigator (CHFI)	Master of Security Science (MSS)

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
Exam Code: 312-50-ANSI (IBT),
312-50v8 (VUE), or 350CEHv8 (APTC)

Start

Attend Training

Prepare for 312-50 Exam

Take Exam

Pass

Certification Achieved

Fail

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

CEHv8 Exam Information

CEH
Certified Ethical Hacker

- ✓ Exam Title:** Certified Ethical Hacker v8 (ANSI)
- ✓ Exam Code:** 312-50-ANSI (IBT), 312-50v8 (VUE), or 350CEHv8 (APTC)
- ✓ Number of Questions:** 125
- ✓ Duration:** 4 hours
- ✓ Availability:** Prometric Prime/ Prometric APTC/ VUE
- ✓ Passing Score:** 70%
- ✓** The instructor will tell you about the exam schedule/exam voucher details for your training
- ✓** This is a **difficult** exam and requires extensive knowledge of CEH Core Modules

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

Student Facilities

CEH
Certified Ethical Hacker

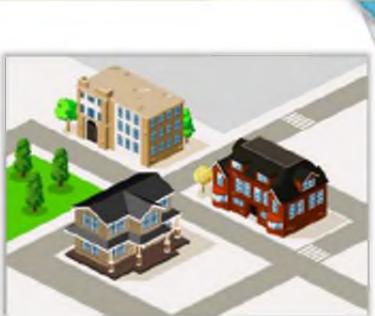
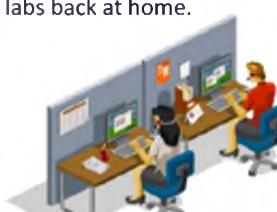
Class Hours		Building Hours		Phones	
	Parking		Messages		Restrooms
Smoking		Meals		Recycling	

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

Lab Sessions

CEH
Certified Ethical Hacker

- 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.



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

What Does CEH Teach You?

CEH
Certified Ethical Hacker



Good Guy
Network Security

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

Ethical Hacking
Bad Guy

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.....

This is What CEH Teaches You!

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

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** class for that

CEH class is 100% NETWORK OFFENSIVE Training Program

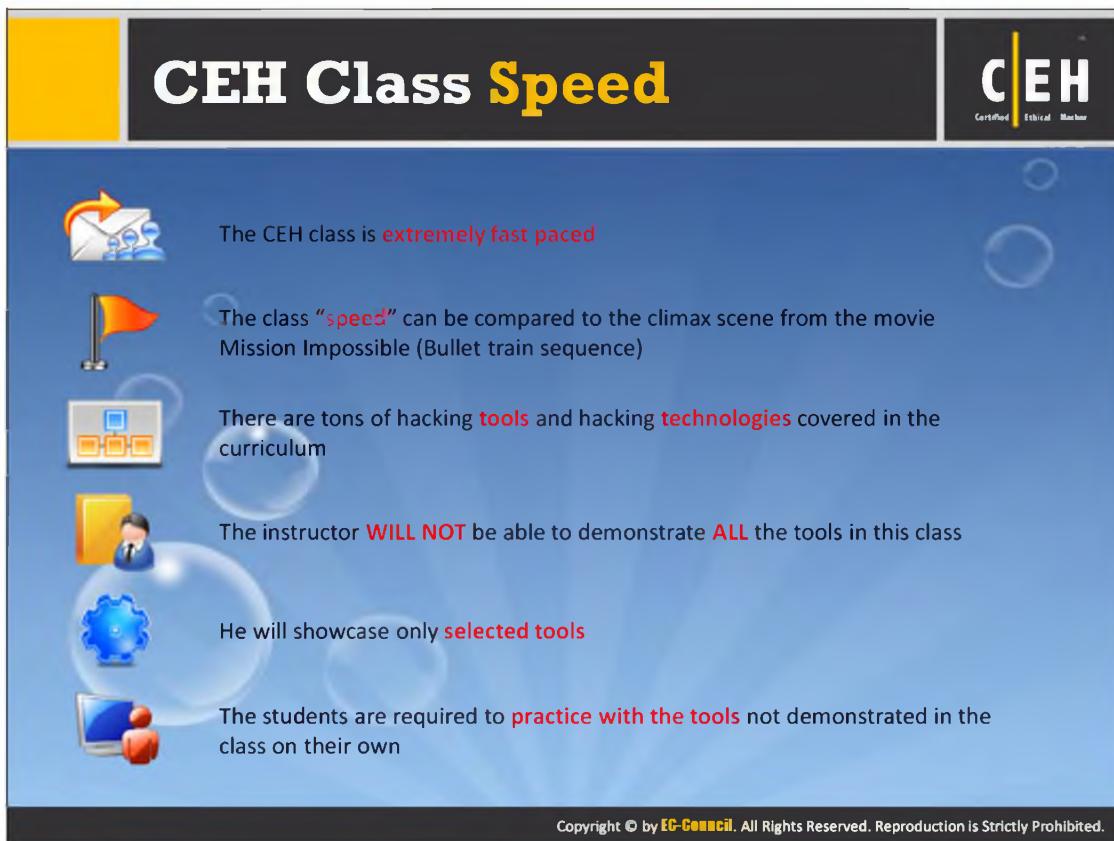
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Remember This!

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

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

CEH Class Speed



The slide features a dark header with a yellow square on the left and the CEH logo on the right. Below the header is a blue background with several icons in bubbles: an envelope, a flag, a server, a folder, a gear, and a computer monitor. To the right of each icon is a statement about the 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

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

Live Hacking Website



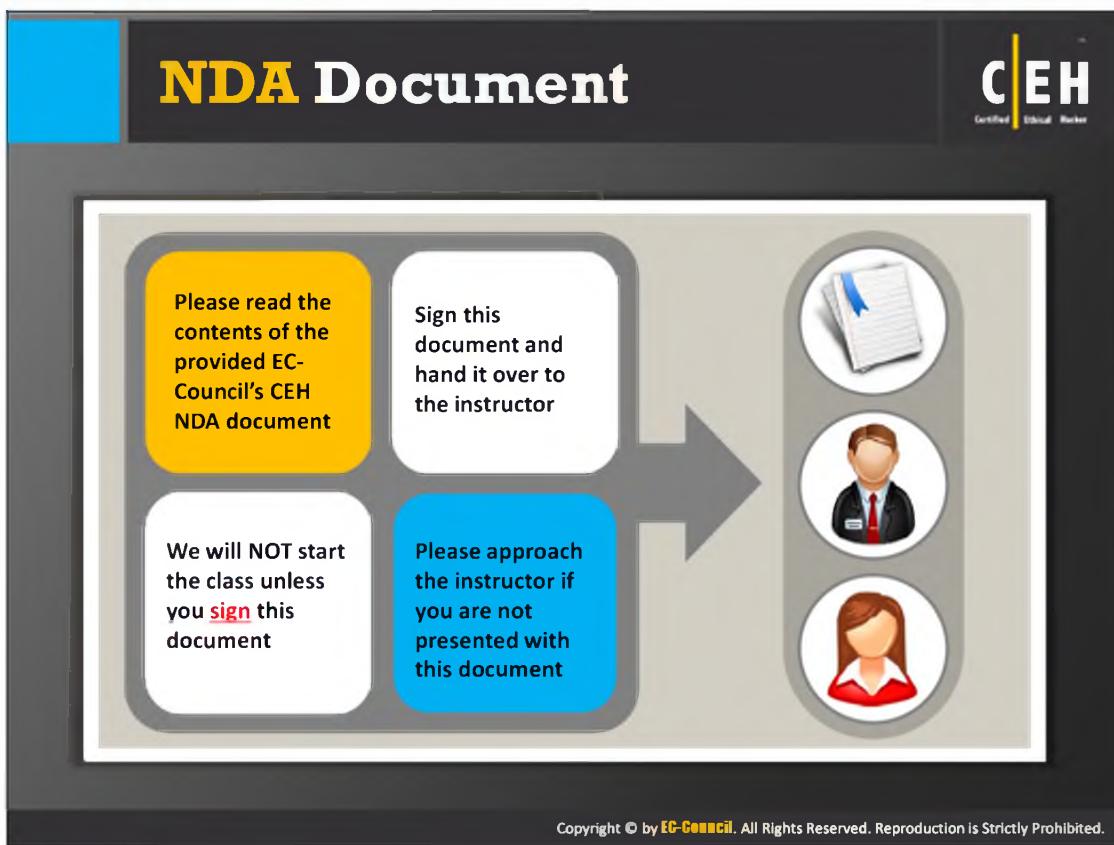
The slide features a dark header with a green square on the left and the CEH logo on the right. Below the header is a white background with a red border around a screenshot of a website. To the right of the screenshot is a small icon of a web browser window. To the right of the browser icon is a red box containing the text "CEH Classroom Attack Lab 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

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

NDA Document

CEH
Certified Ethical Hacker



The slide contains four text boxes and three icons:

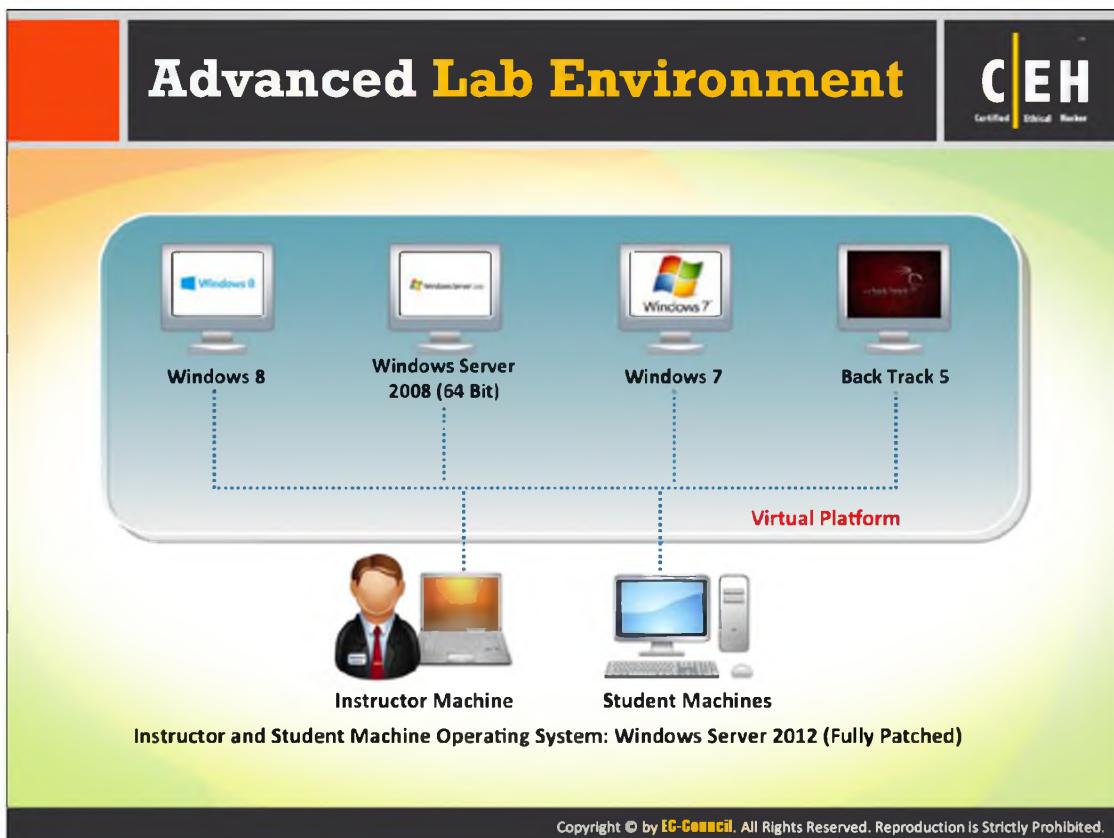
- A yellow box: Please read the contents of the provided EC-Council's CEH NDA document.
- A white box: Sign this document and hand it over to the instructor.
- A grey box: We will NOT start the class unless you **sign** this document.
- A blue box: Please approach the instructor if you are not presented with this document.

Three circular icons on the right represent the Instructor, Male Student, and Female Student.

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

Advanced Lab Environment

CEH
Certified Ethical Hacker



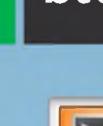
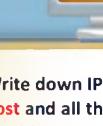
The slide shows a virtual platform with four operating systems: Windows 8, Windows Server 2008 (64 Bit), Windows 7, and Back Track 5. These are connected to an Instructor Machine (laptop) and Student Machines (desktops).

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

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

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 as VM
-  Windows 7 as VM
-  BackTrack 5 R3 as VM

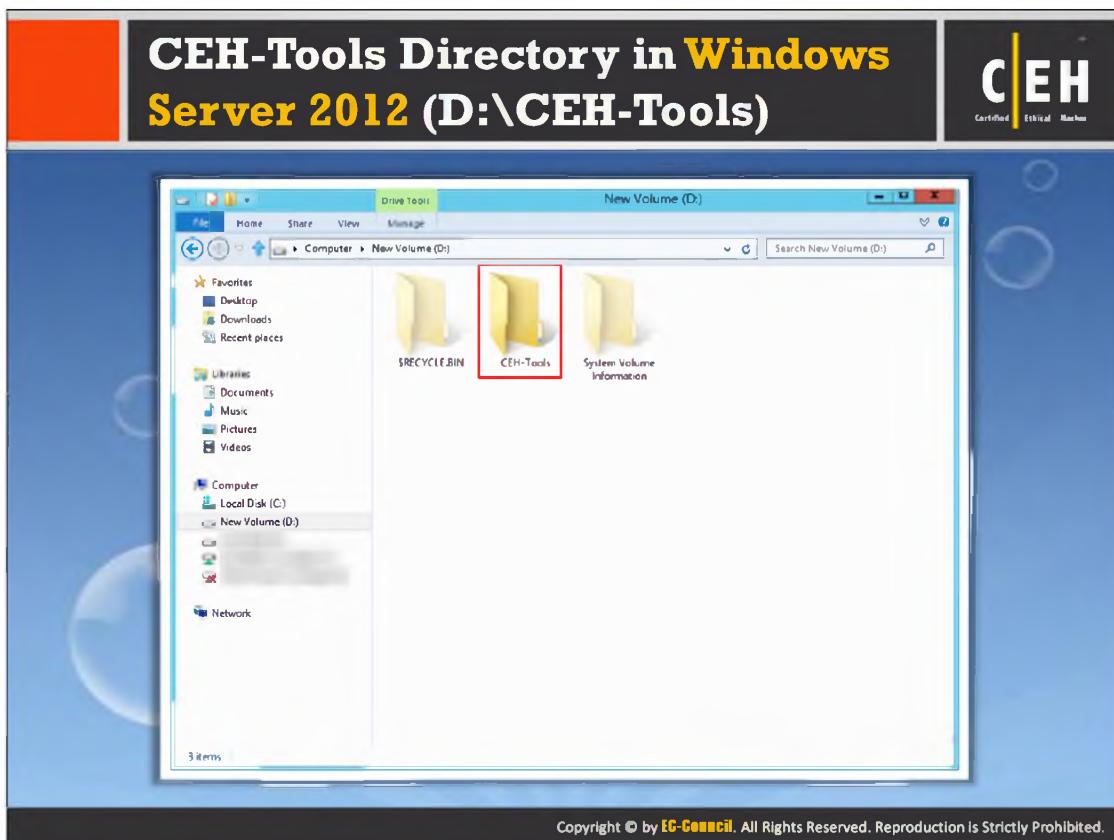
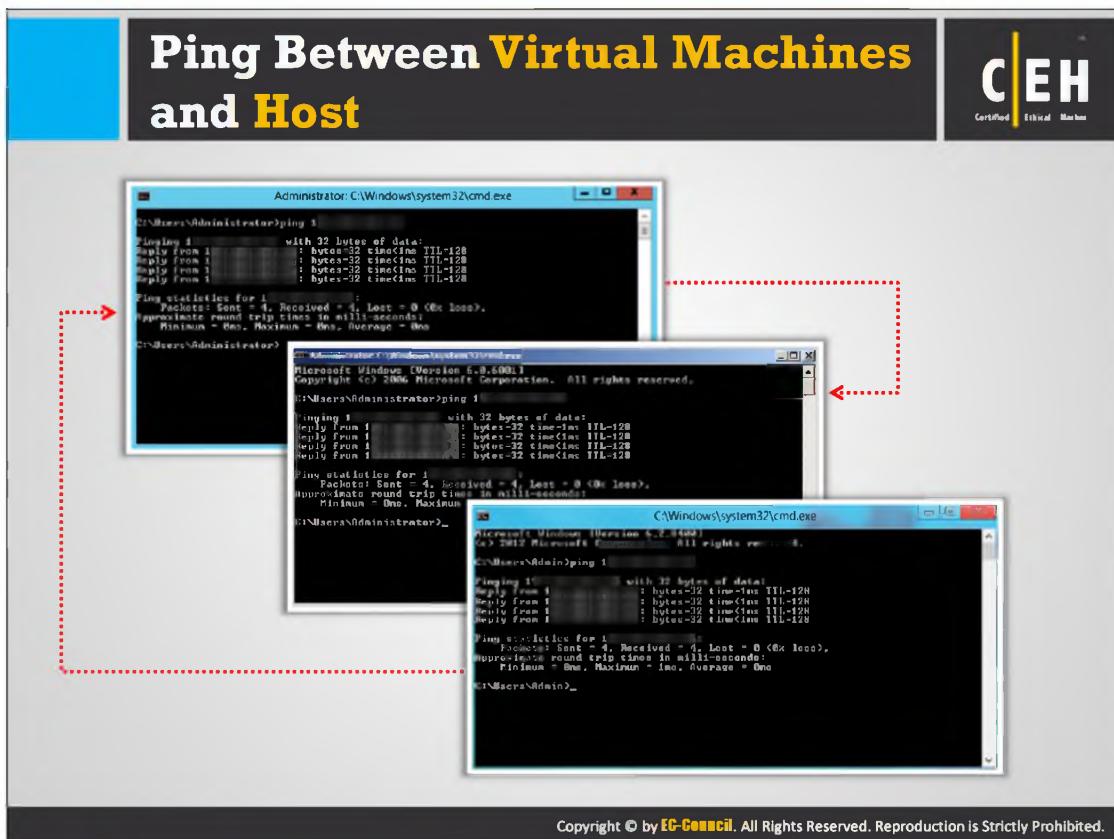
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

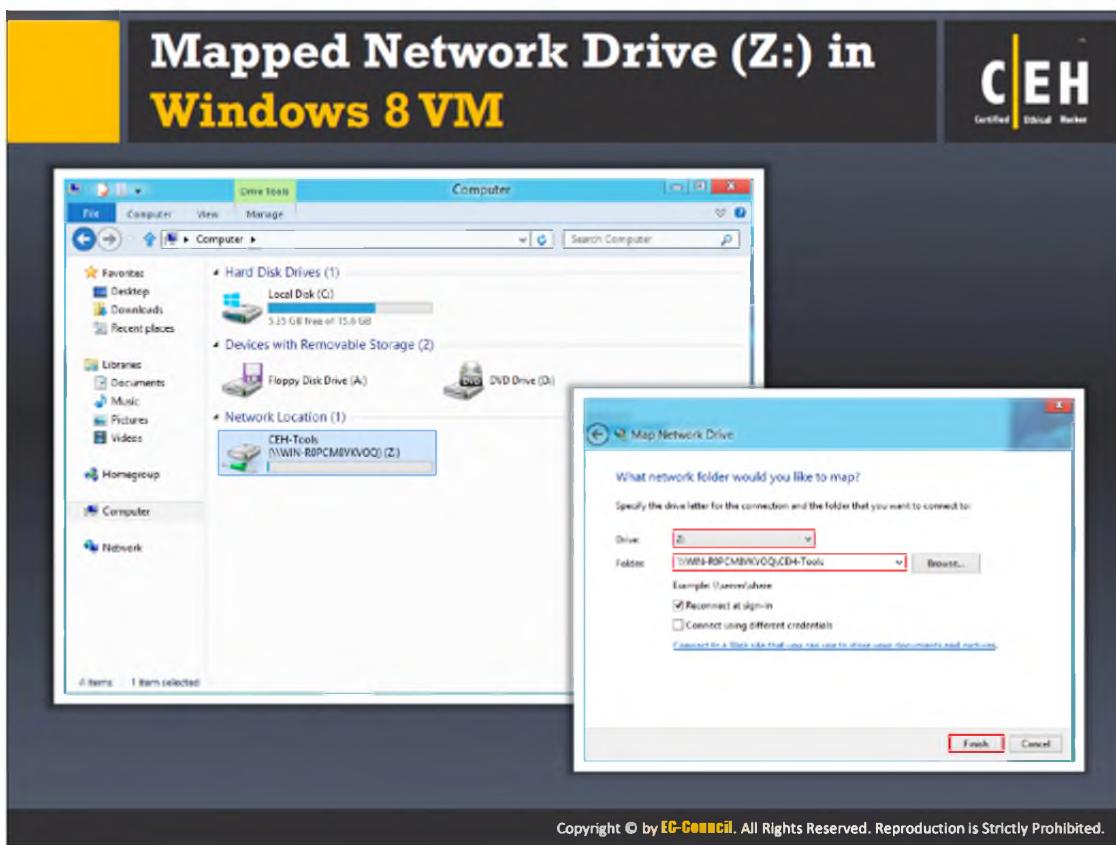
Student Computer Checklist

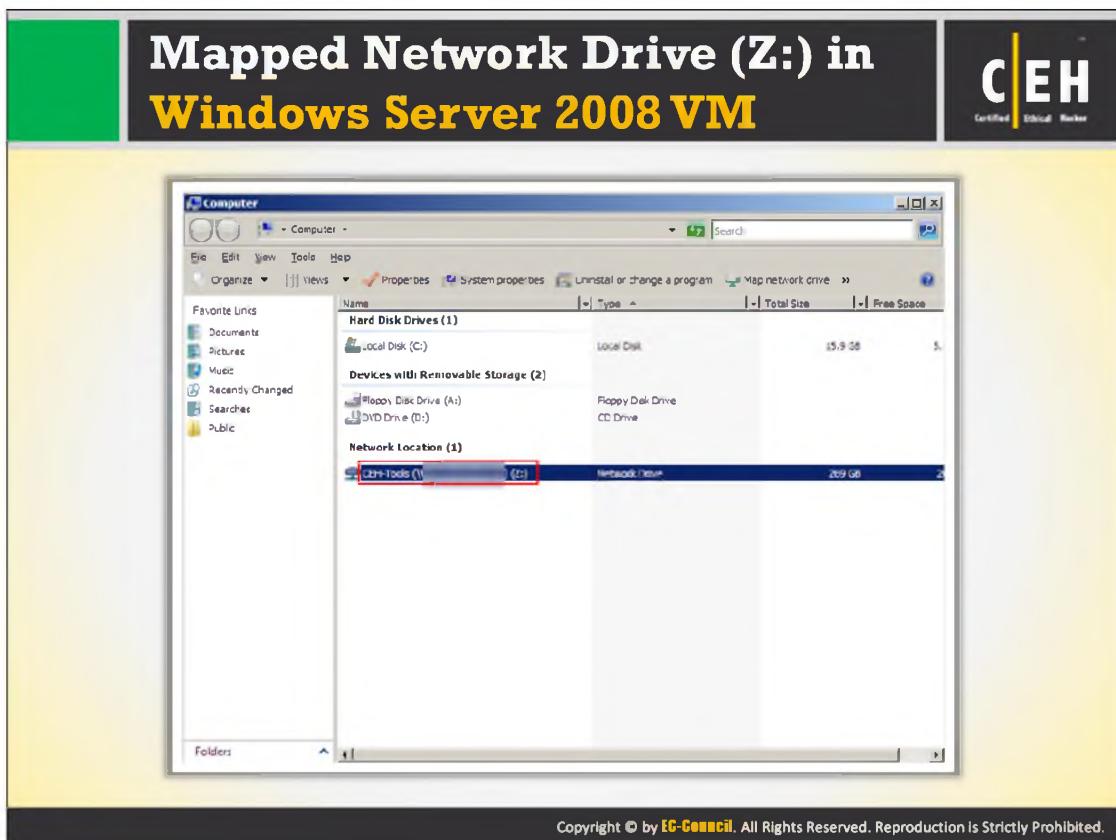
- 1 Write down IP addresses of the **host** and all the **Virtual Machines**
- 2 Check if you can ping between the **VM** and the **hosts**
- 3 Make sure that you can access **D:\CEH-Tools** directory in **Windows Server 2012** and **Z:\CEH-Tools** from all the **VM's**; **Z:** is mapped **Network Drive** 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 **snapshots** of **Virtual Machines**
- 7 For **Wireless Hacking module** you will need **AirPcap adapter**
- 8 Make sure you can access **RealHome** and **Powergym** websites at <http://localhost/realhome> and <http://localhost/powergym>
- 9 Check if you can access <http://www.certifiedhacker.com>

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

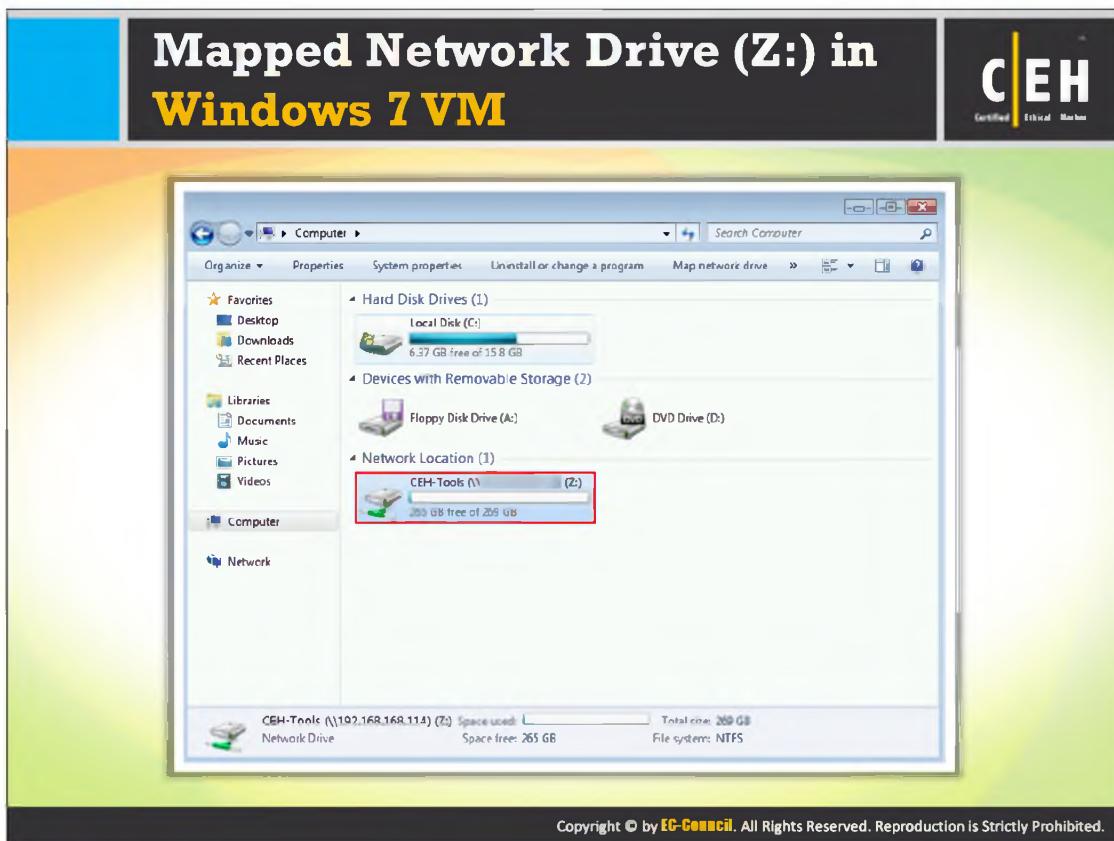




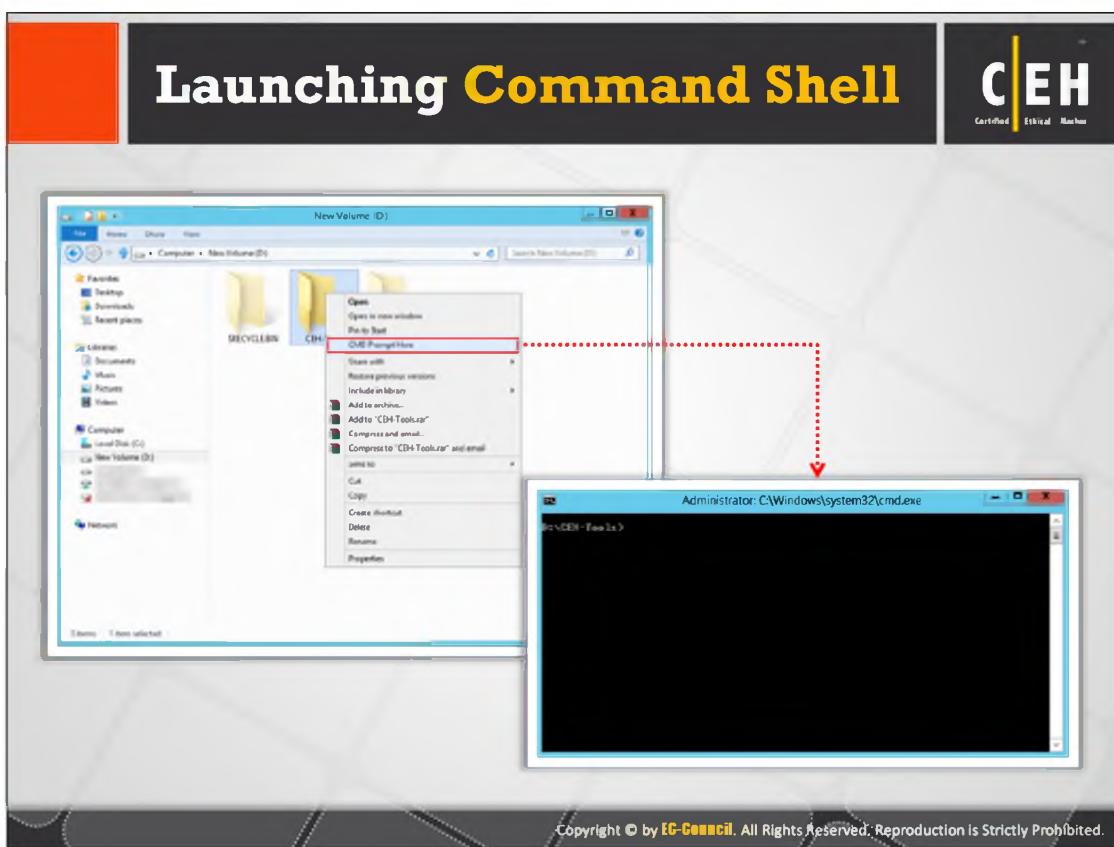
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



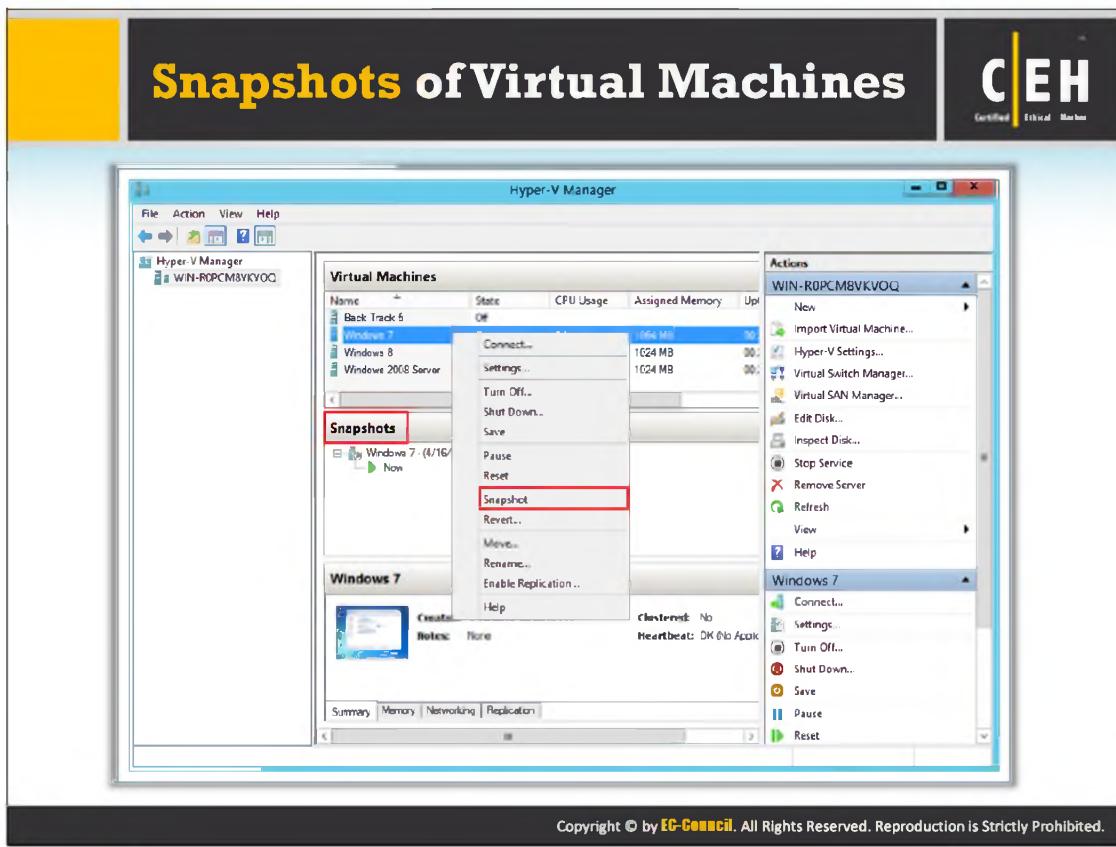
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



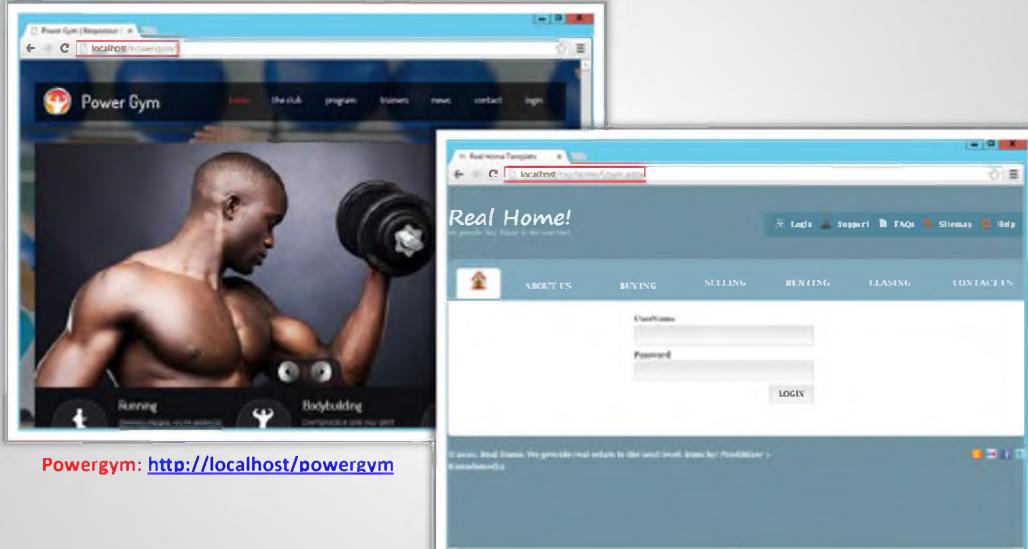
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



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



Powergym and RealHome Websites



The screenshot displays two web browser windows side-by-side. The left window shows the 'Power Gym' website, featuring a muscular man lifting a dumbbell. The right window shows the 'Real Home!' website, which appears to be a login page. Both sites are running on a local host environment.

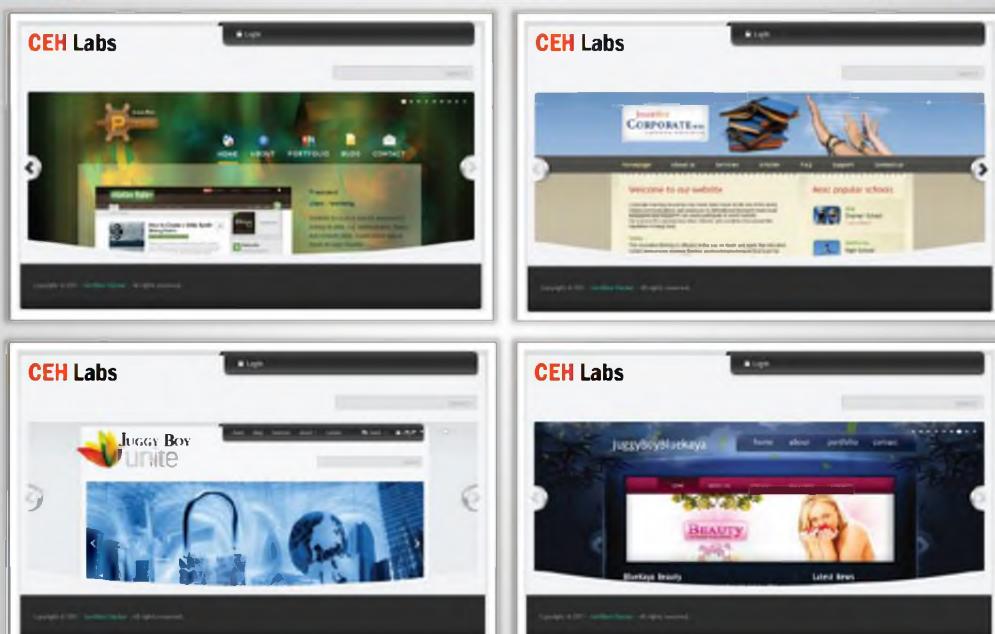
Powergym: <http://localhost/powergym>

RealHome: <http://localhost/realhome>

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

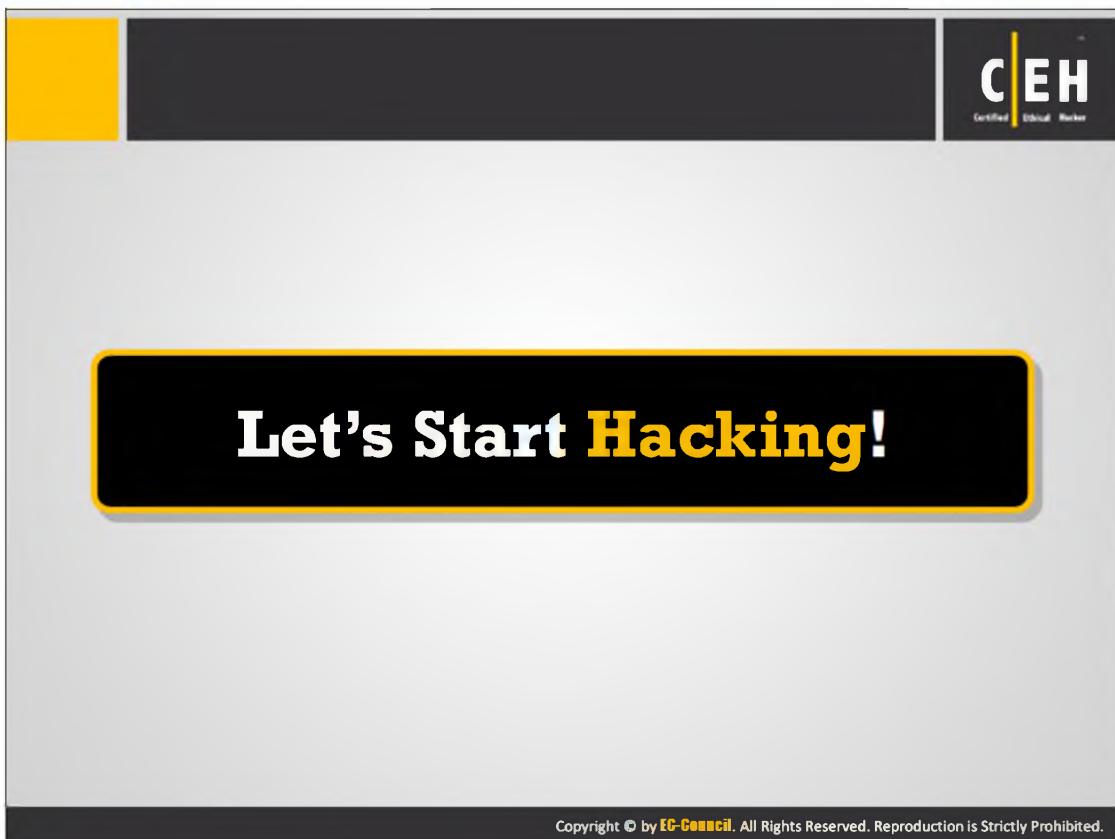
Live Hack Website

<http://www.certifiedhacker.com>



The screenshot shows four separate tabs or windows labeled 'CEH Labs' displaying different website interfaces. The top-left tab shows a landing page for 'Institute CORPORATE'. The top-right tab shows a landing page for 'Institute CORPORATE'. The bottom-left tab shows a landing page for 'Juggy Boy Unite'. The bottom-right tab shows a landing page for 'Blukaya Beauty'. Each tab includes a 'Login' button at the top.

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



Introduction to Ethical Hacking

Module 01



Introduction to Ethical Hacking

Module 01

Engineered by Hackers. Presented by Professionals.



The slide features a dark grey header and footer area. The main title 'Introduction to Ethical Hacking' is in large yellow font. Below it, 'Module 01' is in a smaller white font. The footer contains the text 'Engineered by Hackers. Presented by Professionals.' in white. At the bottom, there is a row of five colored squares containing icons: a black square with 'CEH' and 'Certified Ethical Hacker' text; a green square with a hacker profile icon; a blue square with a computer monitor icon; a yellow square with a ladybug icon; and an orange square with a checkered racing flag icon.

Ethical Hacking and Countermeasures v8

Module 01: Introduction to Ethical Hacking

Exam 312-50

Security News

CEH Certified Ethical Hacker

Home | About Us | Portfolio | Contact Us | Service

Oct 17 2012, 0:45am IST

Zero-day Attacks are Meaner, more Rampant than we ever thought

Computer attacks that target undisclosed vulnerabilities are more common and last longer than many security researchers previously thought. The finding comes from a new study that tracked the number and duration of so-called zero-day exploits over three years.

The typical zero-day attack, by definition, exploits software flaws before they are publicly disclosed. It lasts on average 312 days, with some lasting as long as two and a half years, according to the study by researchers from antivirus provider Symantec. Of the 18 zero-day attacks the researchers found between 2008 and 2011, 11 of them previously went undetected. Recent revelations that the Stuxnet malware that sabotaged Iranian nuclear facilities relied on five zero days already underscored the threat posed by such attacks. But the researchers said their findings suggest the menace may be even greater.

<http://arstechnica.com>

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



News

Zero-day Attacks are Meaner, more Rampant than we ever thought

Source: <http://arstechnica.com>

Computer attacks that target undisclosed vulnerabilities are more common and last longer than many security researchers previously thought. The finding comes from a new study that tracked the number and duration of so-called zero-day exploits over three years.

The typical zero-day attack, by definition, exploits software flaws before they are publicly disclosed. It lasts on average 312 days, with some lasting as long as two and a half years, according to the study by researchers from antivirus provider Symantec. Of the 18 zero-day attacks the researchers found between 2008 and 2011, 11 of them previously went undetected. Recent revelations that the Stuxnet malware that sabotaged Iranian nuclear facilities relied on five zero days already underscored the threat posed by such attacks. But the researchers said their findings suggest the menace may be even greater.

"Zero-day attacks are difficult to prevent because they exploit unknown vulnerabilities, for which there are no patches and no antivirus or intrusion-detection signatures," they wrote. "It seems that, as long as software will have bugs and the development of exploits for new

vulnerabilities will be a profitable activity, we will be exposed to zero-day attacks. In fact, 60 percent of the zero-day vulnerabilities we identify in our study were not known before, which suggests that there are many more zero-day attacks than previously thought—perhaps more than twice as many."

Researchers Leyla Bilge and Tudor Dumitras conducted a systematic study that analyzed executable files collected from **11 million** computers around the world from February 2008 to March 2012. Three of the zero-day exploits they found were disclosed in 2008, seven were disclosed in 2009, six were disclosed in 2010, and two were disclosed in 2011. (The binary reputation data the researchers relied on prevented them from identifying attacks in 2012.) An attack on many versions of Microsoft Windows, which appears to have gone undetected as a zero day until now, had the shortest duration: just 19 days. An exploit of a separate security bug in the Windows shell had the longest duration: 30 months.

Of the 18 attacks studied, 15 targeted 102 or fewer of the 11 million hosts that were monitored. Eight of the exploits were directed at three or fewer hosts. The data confirms conventional wisdom that zero-day attacks are typically reserved for high-value targets. Of the remaining three attacks, one was exploited by Stuxnet and another was exploited by Conficker, the virulent worm discovered in 2008 that has infected millions of computers (and reportedly continues to do so). The Stuxnet and Conficker exploit targeted **1.5 million** and **450,000** hosts respectively. The results, the researchers said, demonstrated the dividends returned by zero-day exploits, which can command prices as high as **\$250,000**.

"For example, Conficker exploiting the vulnerability CVE-2008-4250 managed to infect approximately 370,000 machines without being detected over more than two months," they wrote. "This example illustrates the effectiveness of zero-day vulnerabilities for conducting stealth cyber-attacks."

The researchers cautioned that their method of collecting executable files had significant limitations, causing it to miss 24 zero-day attacks tracked by Symantec's own Internet Security Threats Report over the time period studied. Surprisingly, the number of attacks only grew once zero-day attacks became public knowledge—by margins of two- to 100,000-fold. The number of attack variants also rose, with 183 to 85,000 more variants detected each day. One possible cause of the surge in new files, the researchers said, is that the exploits may have been repackaged versions of the same attack.

"However, it is doubtful that repacking alone can account for an increase by up to five orders of magnitude," they wrote. "More likely, this increase is the result of the extensive re-use of field-proven exploits in other malware."



Copyrights: ©2012 Condé Nast

Author: Dan Goodin

<http://arstechnica.com/security/2012/10/zero-day-attacks-are-meaner-and-more-plentiful-than-thought/>

Module Objectives

C|EH
Certified Ethical Hacker

- Data Breach Investigations Report
- Essential Terminology
- Elements of Information Security
- Top Information Security Attack Vectors
- Information Security Threats
- Hacking vs. Ethical Hacking
- Effects of Hacking on Business
- Who Is a Hacker?

- Hacking Phases
- Types of Attacks on a System
- Why Ethical Hacking Is Necessary
- Skills of an Ethical Hacker
- Incident Management Process
- Types of Security Policies
- Vulnerability Research
- What Is Penetration Testing?



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



Module Objectives

It is important to bear in mind that attackers break into systems for various reasons and purposes. Therefore, it is important to comprehend how **malicious hackers** exploit systems and the probable reasons behind the attacks. As **Sun Tzu** put it in the Art of War, “If you know yourself but not the enemy, for every victory gained, you will also suffer a defeat.” It is the duty of **system administrators** and **network security professionals** to guard their infrastructure against exploits by knowing the enemy—the malicious hacker(s)—who seek to use the same infrastructure for illegal activities.

Ethical hacking is the process of checking and testing the organization network for the possible loopholes and vulnerabilities. The individuals or experts who perform ethical hacking are called **white hats**. They perform hacking in **ethical ways**, without causing any damage to the computer system, thereby **increasing** the **security perimeter** of an organization.

This module covers:

- ⌚ Data Breach Investigations Report
- ⌚ Essential Terminology
- ⌚ Elements of Information Security
- ⌚ Top Information Security Attack Vectors
- ⌚ Information Security Threats
- ⌚ Hacking vs. Ethical Hacking
- ⌚ Effects of Hacking on Business
- ⌚ Who Is a Hacker?
- ⌚ Hacking Phases
- ⌚ Types of Attacks on a System
- ⌚ Why Ethical Hacking Is Necessary
- ⌚ Skills of an Ethical Hacker
- ⌚ Incident Management Process
- ⌚ Types of Security Policies
- ⌚ Vulnerability Research
- ⌚ What Is Penetration Testing?



Module Flow

Information security refers to protecting or safeguarding any kind of sensitive information and information systems from unauthorized access, disclosure, alteration, disruption, and destruction. For most organizations, information is the critical resource to be secured. If sensitive information falls into wrong hands, then the respective organization may face a great threat. In an attempt to understand how to secure such critical information resources, first we will look at an **overview of information security**.

 Information Security Overview	 Hacking Phases
 Information Security Threats and Attack Vectors	 Types of Attacks
 Hacking Concepts	 Information Security Controls

This section covers elements of information security, the strength of the component triangle (security, functionality, and usability), and essential terminology.

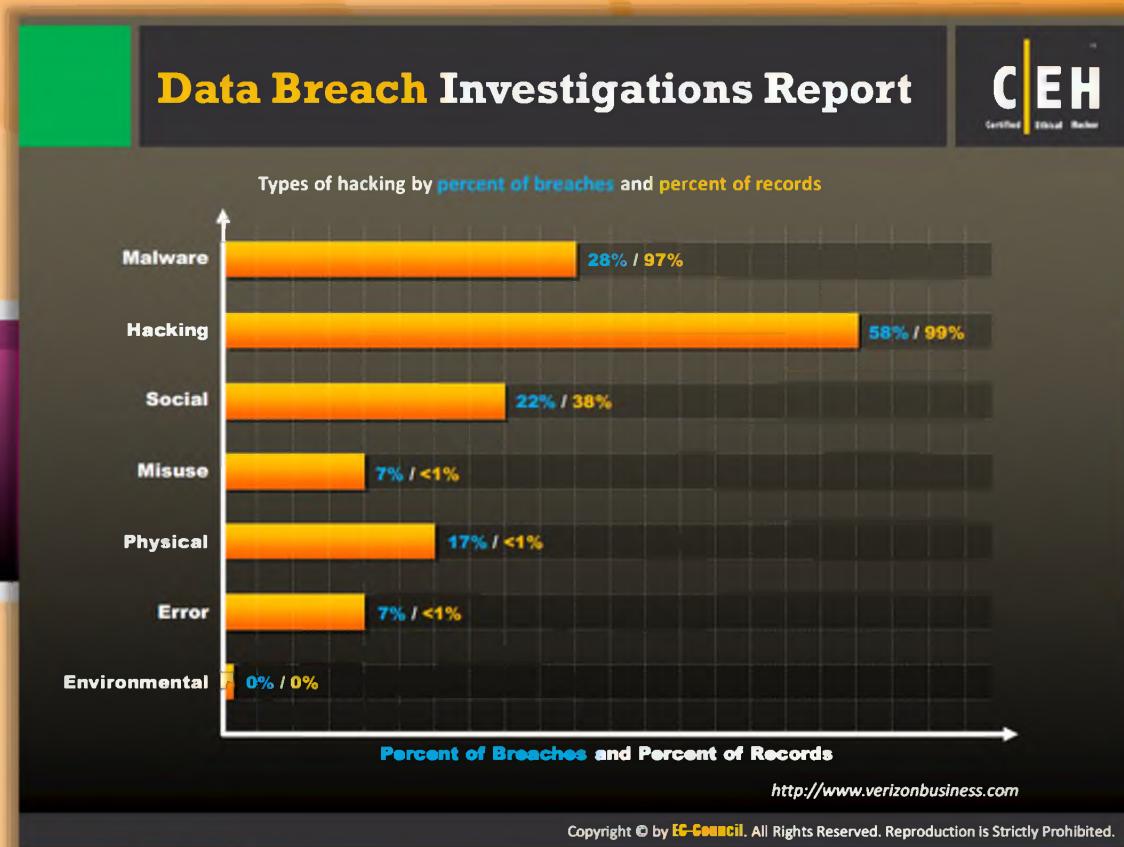


Internet Crime Current Report: IC3

Source: <http://www.ic3.gov>

The following is the crime report data from IC3; the **Internet Crime Complaint Center (IC3)** is a partnership among the Federal Bureau of Investigation (**FBI**), the National White Collar Crime Center (**NW3C**), and the Bureau of Justice Assistance (**BJA**). According to IC3, online Internet crime complaints are increasing daily. From the graph, you can observe that in the year **2005**, there were **231,493 crime complaints**, whereas in the year **2009**, complaints drastically increased to **336,655**. When compared to 2009, Internet crime complaints in the year **2011 decreased** to some extent.





Data Breach Investigations Report

Source: <http://www.verizonbusiness.com>

The data breach investigations report from **Verizon Business** shows the types of hacking by percent of breaches and percent of records. From the report, it is clear that most of the security breaches happening today are because of **hacking**. Therefore, in order to protect yourself from data or **security breaches**, you should test your network security against hacking.

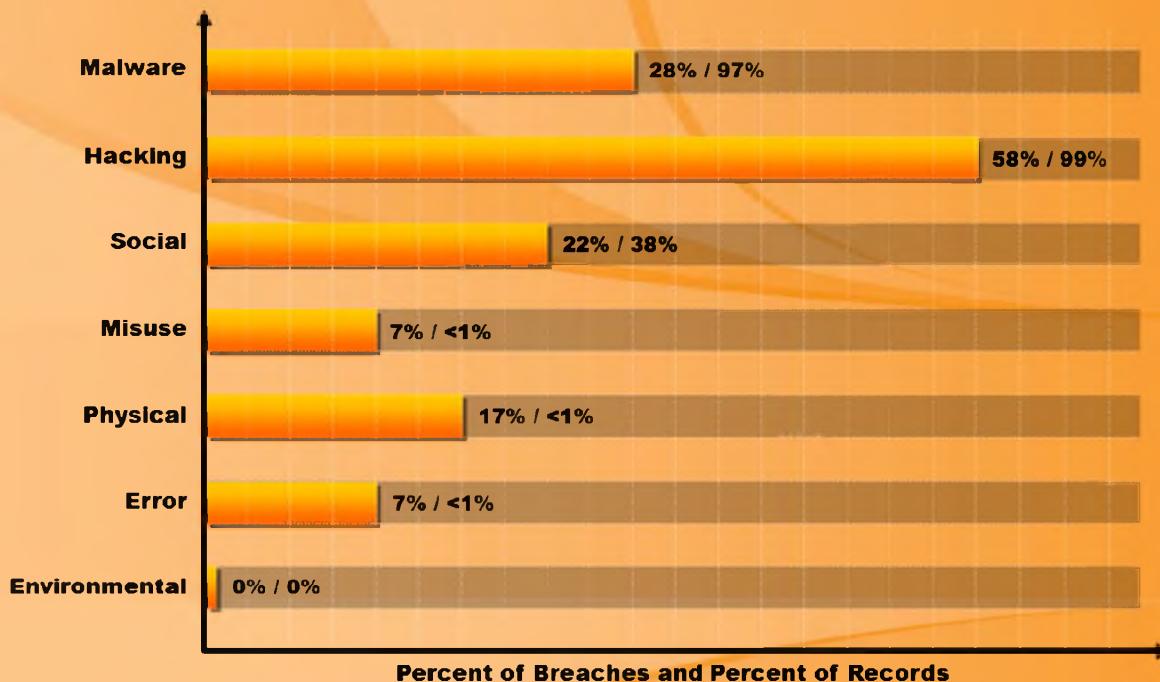


FIGURE 1.1: Data Breach Investigation Report

Essential Terminology

C|EH
Certified Ethical Hacker

Hack Value  It is the notion among hackers that something is worth doing or is interesting	Target of Evaluation  An IT system, product, or component that is identified/subjected to a required security evaluation
Exploit  A defined way to breach the security of an IT system through vulnerability	Zero-Day Attack  An attack that exploits computer application vulnerabilities before the software developer releases a patch for the vulnerability
Vulnerability  Existence of a weakness, design, or implementation error that can lead to an unexpected and undesirable event compromising the security of the system	Daisy Chaining  Hackers who get away with database theft usually complete their task, then backtrack to cover their tracks by destroying logs, etc.

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

Essential Terminology



Hack Value

Hack value is the notion among hackers that something is worth doing or is interesting. Hackers might feel that **breaking down** the toughest network security might give them great satisfaction, and that it is something they accomplished that not everyone could do.



Exploit

An exploit is a defined way to **breach** the **security** of an IT system through vulnerability. The term exploit is used when any kind of attack has taken place on a system or network. An exploit can also be defined as **malicious software** or **commands** that can cause unanticipated behavior to occur on **legitimate software** or **hardware** by taking advantage of the vulnerabilities.



Vulnerability

Vulnerability is a **weakness in design** or an **implementation error** that can lead to an unexpected and undesirable event compromising the **security of the system**. In simple words, a vulnerability is **loop hole**, **limitation**, or **weakness** that becomes a source for an attacker to enter into the system by **bypassing** various user authentications.



Target of Evaluation

A target of evaluation is an IT system, product, or component that is identified / subjected to a required security evaluation. This kind of evaluation helps the evaluator understand the functioning, technology, and vulnerabilities of a particular system or product.



Zero-day Attack

In a zero-day attack, the **attacker exploits the vulnerabilities** in the computer application before the software developer releases a patch for them.



Daisy Chaining

Attackers who get away with **database theft** usually complete their task and then **backtrack** to cover their tracks by **destroying logs**, etc. The attackers gain control of other systems and use them for malicious activities. It becomes difficult to identify the attacker as they use others' systems to perform illegal activities.

Elements of Information Security

A state of well-being of information and infrastructure in which the possibility of **theft**, **tampering**, and **disruption of information and services** is kept low or tolerable

The diagram illustrates the five elements of information security as a sequence of five arrows pointing from left to right. Each arrow contains a brief definition and an associated icon.

- Confidentiality:** Assurance that the information is accessible only to those authorized to have access. Icon: A folder with a green lock and a keyhole.
- Integrity:** Assurance that the systems responsible for delivering, storing, and processing information are accessible when required by the authorized users. Icon: A document with a green checkmark.
- Availability:** Guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message. Icon: A document with a green checkmark.
- Authenticity:** The trustworthiness of data or resources in terms of preventing improper and unauthorized changes. Icon: A document with a green checkmark.
- Non-Repudiation:** Authenticity refers to the characteristic of a communication, document or any data that ensures the quality of being genuine. Icon: A person in a green hoodie.

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



Elements of Information Security

Information security is defined as: "A state of well-being of **information** and **infrastructure** in which the possibility of theft, tampering, and disruption of information and services is kept low or tolerable." It relies on the five major elements of: **confidentiality**, **integrity**, **availability**, **authenticity**, and **non-repudiation**.



Confidentiality

Confidentiality is the assurance that the information is accessible only to those authorized to have access. Confidentiality breaches may occur due to improper data handling or a **hacking attempt**.



Integrity

Integrity is the trustworthiness of data or resources in terms of preventing **improper** and **unauthorized changes**, the assurance that information can be relied upon to be sufficiently accurate for its purpose.



Availability

Availability is the assurance that the systems responsible for delivering, storing, and

processing information are accessible when required by authorized users.



Authenticity

Authenticity refers to the characteristic of a communication, document, or any data that ensures the **quality** of being **genuine** or not corrupted from the original. The major roles of authentication include confirming that the user is who he or she claims to be and ensuring the message is **authentic** and **not altered or forged**. Biometrics, smart cards, and **digital certificates** are used to ensure authenticity of data, transactions, communications, or documents.



Non-repudiation

Non-repudiation refers to the ability to ensure that a party to a contract or a communication cannot deny the **authenticity** of their **signature** on a document or the sending of a message that they originated. It is a way to guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message.

The Security, Functionality, and Usability Triangle

Level of security in any system can be defined by the strength of three components:

Moving the ball towards security means less functionality and usability

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



The Security, Functionality, and Usability Triangle

Technology is evolving at an unprecedented rate. As a result, new products that reach the market tend to be engineered for easy-to-use rather than secure computing. Technology, originally developed for “honest” **research** and **academic purposes**, has not evolved at the same pace as the user’s profile. Moreover, during this evolution, system designers often overlook the vulnerabilities during the intended deployment of the system. However, increasing built-in default **security mechanisms** means users have to be more competent. As computers are used for more and more routine activities, it is becoming increasingly difficult for system administrators and other system professionals to allocate resources exclusively for securing systems. This includes time needed to **check log files**, **detect vulnerabilities**, and **apply security update patches**.

Routine activities consume system administrators’ time, leaving less time for vigilant administration. There is little time to deploy measures and secure computing resources on a regular and innovative basis. This has increased the demand for dedicated security professionals to constantly monitor and defend **ICT (Information and Communication Technology)** resources.

Originally, to “hack” meant to possess extraordinary computer skills to extend the limits of computer systems. Hacking required **great proficiency**. However, today there are automated

tools and codes available on the Internet that make it possible for anyone with a will and desire to hack and succeed.

Mere compromise of the security of a system does not denote success. There are websites that insist on “**taking back the net**” as well as people who believe that they are doing all a favor by posting exploit details. These can act as a detriment and can bring down the skill level required to become a successful attacker.

The ease with which system vulnerabilities can be exploited has increased while the knowledge curve required to perform such exploits has shortened. The concept of the elite/super attacker is an illusion. However, the fast-evolving genre of “**script kiddies**” is largely comprised of lesser-skilled individuals having **second-hand knowledge** of performing exploits. One of the main impediments contributing to the growth of **security infrastructure** lies in the unwillingness of exploited or compromised victims to report the incident for fear of losing the goodwill and faith of their employees, customers, partners, and/or of losing market share. The trend of information assets influencing the market has seen more companies thinking twice before **reporting incidents** to law enforcement for fear of bad press and negative publicity.

The increasingly networked environment, with companies often having their website as a single point of contact across geographical boundaries, makes it critical for administrators to take countermeasures to prevent **exploits** that can result in loss of an important reason why corporations need to invest in **security measures** to protect their information assets.



Module Flow

So far we discussed information security. Now we will discuss **threats** and **attack vectors** of information security.

 Information Security Overview	 Hacking Phases
 Information Security Threats and Attack Vectors	 Types of Attacks
 Hacking Concepts	 Information Security Controls

This section introduces you to top information security attack vectors, the possible **security threats** to valuable information, and the **goals of attackers** who perform attacks on information systems.



Top Information Security Attack Vectors

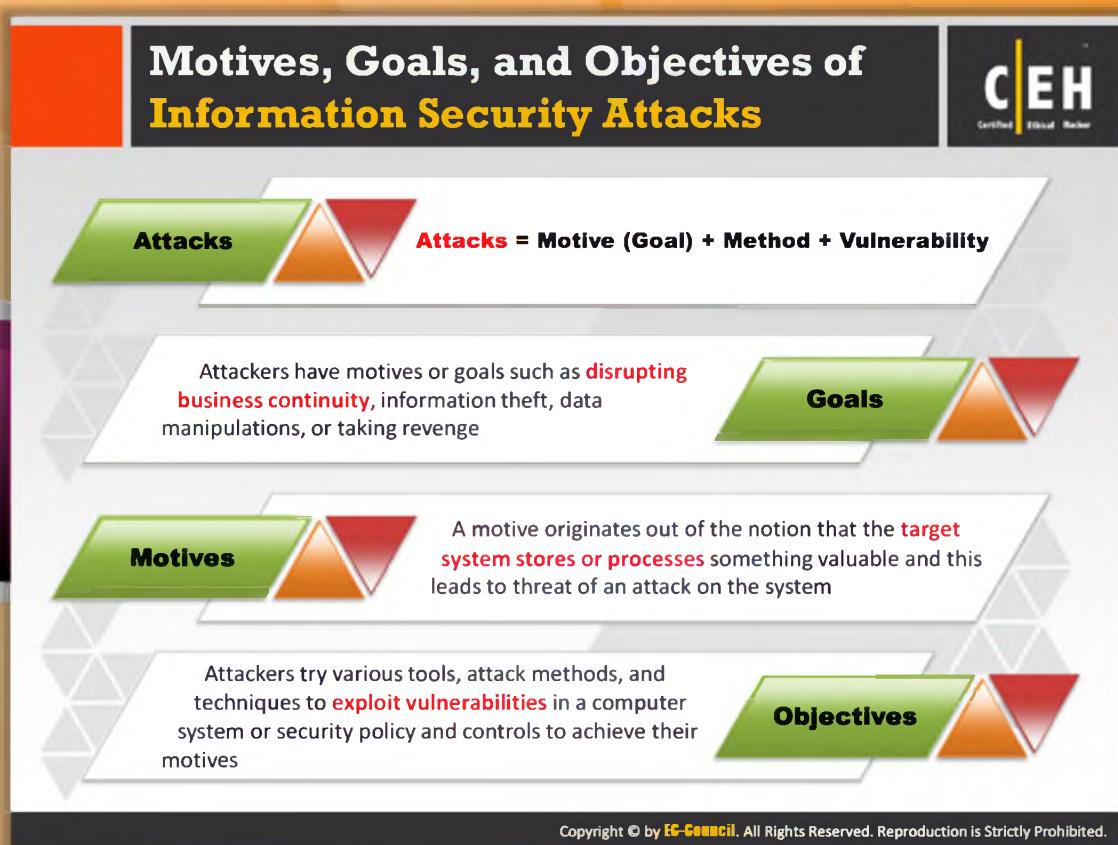
An attack vector is a path or means by which an attacker gains access to an information system to **perform malicious activities**. This attack vector enables an attacker to take advantage of the vulnerabilities present in the **information system** in order to carry out a particular attack.

Although there are some **traditional attacks vectors** from which attack can be performed, attack vectors come in many forms; one cannot predict in which form an attack vector can come.

The following are the **possible top attack vectors** through which attackers can attack information systems:

- ⌚ Virtualization and Cloud Computing
- ⌚ Organized Cyber Crime
- ⌚ **Unpatched Software**
- ⌚ Targeted Malware
- ⌚ Social Networking
- ⌚ Insider Threats

- ⌚ **Botnets**
- ⌚ Lack of Cyber Security Professionals
- ⌚ Network Applications
- ⌚ Inadequate Security Policies
- ⌚ Mobile Device Security
- ⌚ Compliance with Govt. Laws and Regulations
- ⌚ Complexity of Computer Infrastructure
- ⌚ **Hacktivism**



Motives, Goals, and Objectives of Information Security Attacks

Attackers generally have motives or **goals or objectives** behind performing information security attacks. It may be to disrupt the **business continuity** of the target organization, to **steal** valuable **information**, for the sake of **curiosity**, or even to take **revenge** on target organization. Therefore, these motives or goals depend on the attacker's state of mind, for what reason he or she is carrying out such an activity. Once, the attacker determines his/her **goal**, he or she can accomplish the goal by adopting various techniques to exploit vulnerabilities in an **information system** or **security policy** and controls.

Information Security Threats

C|EH
Certified Ethical Hacker

Natural Threats

- Natural disasters
- Floods
- Earthquakes
- Hurricanes



Physical Security Threats

- Loss or damage of system resources
- Physical intrusion
- Sabotage, espionage and errors



Human Threats

- Hackers
- Insiders
- Social engineering
- Lack of knowledge and awareness



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



Information Security Threats

Information security threats are broadly classified into **three** categories, as follows:



Natural Threats

Natural threats include **natural disasters** such as earthquakes, hurricanes, floods, or any **nature-created disaster** that cannot be stopped. Information damage or loss due to natural threats cannot be prevented as no one knows in advance that these types of threats will occur. However, you can implement a few **safeguards** against natural disasters by adopting **disaster recovery plans** and **contingency plans**.



Physical Security Threats

Physical threats may include loss or damage of **system resources** through fire, water, theft, and **physical impact**. Physical impact on resources can be due to a **collision** or other damage, either intentionally or unintentionally. Sometimes, power may also damage hardware used to store information.



Human Threats

Human threats include threats of attacks performed by **both insiders and outsiders**.

Insider attacks refer to attacks performed by **disgruntled** or malicious **employees**. Outsider attacks refer to attacks performed by **malicious people** not within the organization. **Insider** attackers can be the **biggest threat** to information system as they may know the **security posture** of the information system, while **outsider** attackers apply many tricks such as **social engineering** to learn the security posture of the information system.



Information Security Threats (Cont'd)

Human threats can be further classified into **three types**, as follows:



Network Threats

A network is defined as the **collection of computers and other hardware** connected by communication channels to share resources and information. As the information travels from one computer to the other through the **communication channel**, a malicious person may break into the communication channel and **steal** the **information** traveling over the network. The attacker can impose various threats on a target network:

- Information gathering
- Sniffing and eavesdropping
- Spoofing**
- Session hijacking and man-in-the-middle attacks
- SQL injection
- ARP Poisoning**
- Password-based attacks

- ⌚ Denial of service attack
- ⌚ Compromised-key attack



Host Threats

Host threats are directed at a particular system on which valuable information resides. Attackers try to breach the security of the **information system resource**. The following are possible threats to the host:

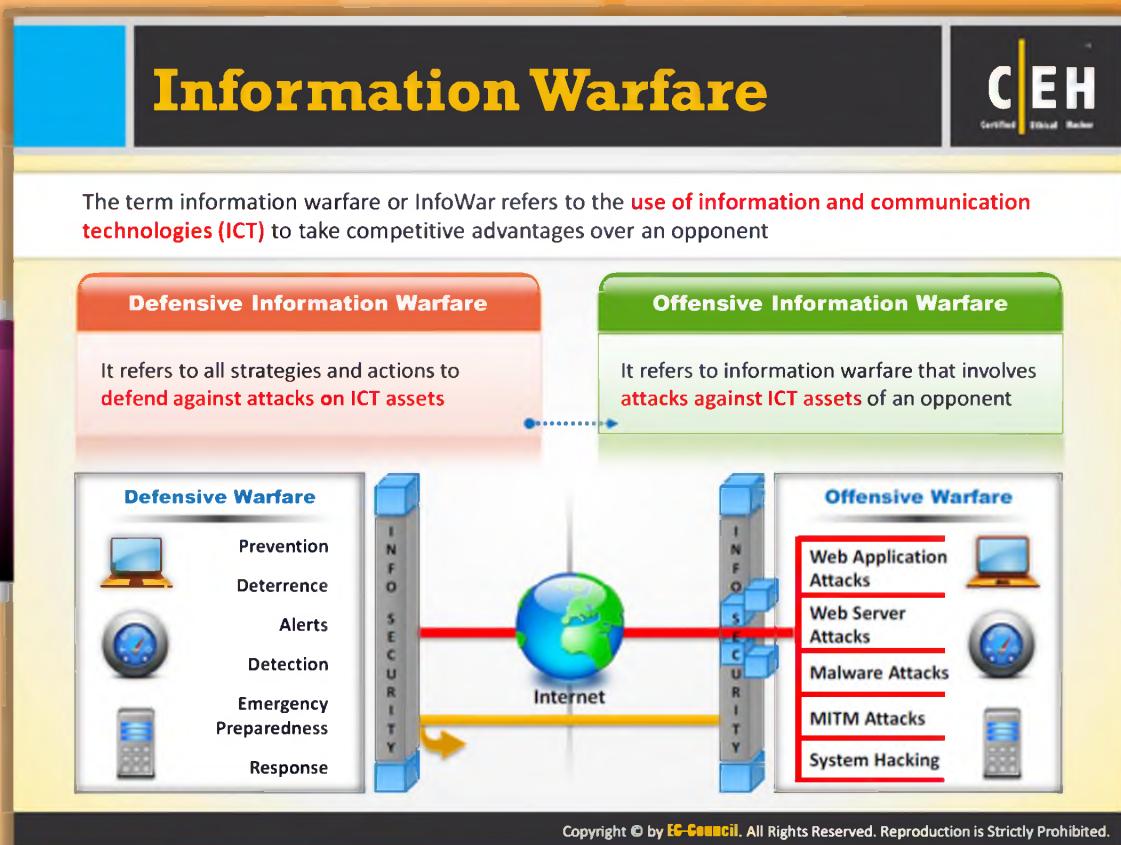
- ⌚ Malware attacks
- ⌚ Target **Footprinting**
- ⌚ Password attacks
- ⌚ Denial of service attacks
- ⌚ Arbitrary code execution
- ⌚ **Unauthorized access**
- ⌚ Privilege escalation
- ⌚ **Back door** Attacks
- ⌚ Physical security threats



Application Threats

If the proper **security measures** are not considered during **development** of the particular **application**, the application might be vulnerable to different types of application attacks. Attackers take advantage of **vulnerabilities** present in the application to **steal** or **damage** the information. The following are possible threats to the application:

- ⌚ Data/Input validation
- ⌚ Authentication and Authorization attacks
- ⌚ Configuration **management**
- ⌚ Information disclosure
- ⌚ Session management issues
- ⌚ Buffer overflow issues
- ⌚ Cryptography attacks
- ⌚ Parameter **manipulation**
- ⌚ Improper error handling and exception management
- ⌚ Auditing and logging issues



Information Warfare

The term information warfare or **InfoWar** refers to the use of information and **communication technologies (ICT)** to take **competitive advantages** over an opponent.

Defensive Information Warfare: It refers to all strategies and actions to defend against attacks on ICT assets.

Offensive Information Warfare: It refers to information warfare that involves attacks against **ICT assets** of an opponent.

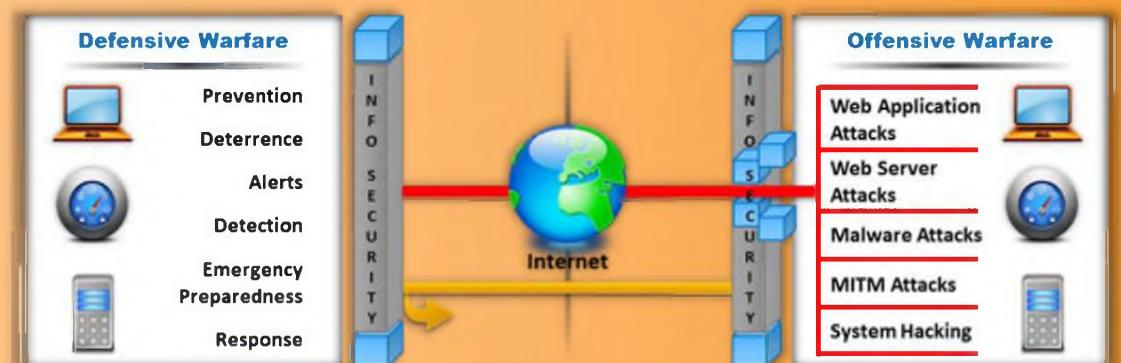


FIGURE 1.2: Defensive and Offensive Warfare Diagram

IPv6 Security Threats

C|EH
Certified Ethical Hacker

- Auto Configuration Threats**
IPv6 enables auto-configuration of IP networks, which may leave user **vulnerable to attacks** if the network is not configured properly and securely from the very beginning
- Unavailability Reputation-based Protection**
Current security solutions use reputation of IP addresses to **filter out known sources of malware**; vendors will take time to develop reputation-based protection for IPv6
- Incompatibility of Logging Systems**
IPv6 uses 128-bit addresses, which are stored as a **39-digit string** whereas IPv4 addresses stored in a **15-character field**; logging solutions designed for IPv4 may not work on IPv6 based networks
- Rate Limiting Problem**
Administrators use **rate limiting strategy** to slow down the automated attack tool; however, it is impractical to rate limit at the 128-bit address level

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



IPv6 Security Threats

Compared to IPv4, IPv6 has an **improved security** mechanism that assures a higher level of security and confidentiality for the information transferred over a network. However, IPv6 is still vulnerable. It still possesses information security threats that include:



Auto Configuration Threats

IPv6 enables auto-configuration of IP networks, which may leave user vulnerable to attacks if the network is not configured properly and securely from the beginning.



Unavailability Reputation-based Protection

Current security solutions use the reputation of IP addresses to filter out known sources of malware; vendors will take time to develop **reputation-based protection** for IPv6.



Incompatibility of Logging Systems

IPv6 uses 128-bit addresses, which are stored as a **39-digit string**, whereas IPv4 addresses are stored in a **15-character field**; logging solutions designed for IPv4 may not work on IPv6-based networks.



Rate Limiting Problem

Administrators use a rate limiting strategy to slow down the automated attack tool; however, it is impractical to rate limit at the 128-bit address level.

IPv6 Security Threats (Cont'd)



Default IPv6 Activation
IPv6 may be activated without administrator's knowledge, which will leave IPv4-based security controls ineffective

Complexity of Network Management Tasks
Administrators may adopt easy-to-remember addresses (::10, ::20, ::F00D, ::C5C0 or simply IPv4 last octet for dual stack) leading to potential vulnerability

Overloading of Perimeter Security Controls
IPv6 has a 40-byte fixed header with an add-on "extension header" that may be chained, which require a complex processing by various security controls systems such as routers, security gateways, firewalls and IDSes

Complexity in Vulnerability Assessment
IPv6's 128-bit address space makes active scanning of infrastructure for unauthorized or vulnerable systems more complex

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



IPv6 Security Threats (Cont'd)

You may also find the following threats when using IPv6:



Default IPv6 Activation

IPv6 may be activated without the administrator's knowledge, which will leave IPv4-based security controls ineffective.



Complexity of Network Management Tasks

Administrators may adopt easy-to-remember addresses (::10, ::20, ::F00D, ::C5C0 or simply IPv4 last octet for dual stack) leading to a potential vulnerability.



Complexity in Vulnerability Assessment

IPv6's 128-bit address space makes active scanning of infrastructure for unauthorized or vulnerable systems more complex.



Overloading of Perimeter Security Controls

IPv6 has a 40-byte fixed header with an add-on "extension headers" that may be chained, which requires complex processing by various security controls systems such as routers, security gateways, firewalls, and IDS.

IPv6 Security Threats (Cont'd)



IPv4 to IPv6 Translation Issues
Translating IPv4 traffic to IPv6 may result in a poor implementation and may provide a potential attack vector

Security Information and Event Management (SIEM) Problems
Every IPv6 host can have multiple IPv6 addresses simultaneously, which leads to complexity of log or event correlation

Denial-of-Service (DoS)
Overloading of network security and control devices can significantly reduce the availability threshold of network resources leading to DoS attacks

Trespassing
IPv6's advanced network discovery features can be exploited by attackers traversing through your network and accessing the restricted resources

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



IPv6 Security Threats (Cont'd)

The following IPv6 security threats can also cause **serious damage** to your network:



IPv4 to IPv6 Translation Issues

Translating IPv4 traffic to IPv6 may result in **poor implementation** and may provide a potential attack vector.



Security Information and Event Management (SIEM) Problems

Every IPv6 host can have multiple IPv6 addresses simultaneously, which leads to **complexity of log or event correlation**.



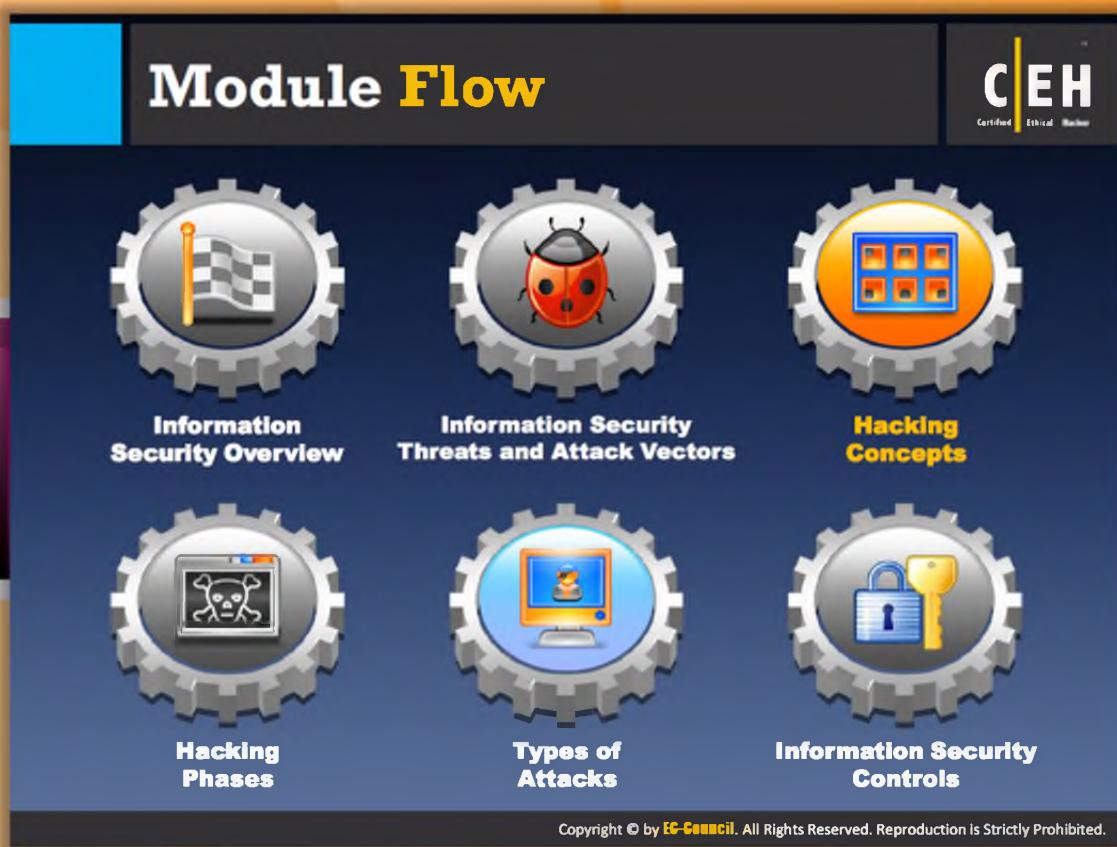
Denial-of-service (DoS)

Overloading of network security and **control devices** can significantly reduce the availability threshold of network resources, leading to DoS attacks.



Trespassing

IPv6's advanced network discovery features can be exploited by attackers who can traverse through your network and access the **restricted resources**.



Module Flow

So far we have discussed **information security**, its **threats** and attack vectors. Now we will discuss how an attacker compromises information security with the help of **attack vectors**.

Information Security Overview	Hacking Phases
Information Security Threats and Attack Vectors	Types of Attacks
Hacking Concepts	Information Security Controls

This section will familiarize you with the **concept of ethical hacking**, how it differs from hacking, the **effects** of hacking activities on business, and different **classes of attackers**.

Hacking vs. Ethical Hacking

C|EH
Certified Ethical Hacker

- Hacking refers to **exploiting system vulnerabilities** and **compromising security controls** to gain unauthorized or inappropriate access to the system resources
- It involves **modifying system or application features** to achieve a goal outside of the creator's original purpose

- Ethical hacking involves the use of hacking tools, tricks, and techniques to **identify vulnerabilities** so as to ensure system security
- It focuses on simulating techniques used by attackers to **verify the existence of exploitable vulnerabilities** in the system security

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



Hacking vs. Ethical Hacking

Most people do not understand the difference between hacking and ethical hacking. These two terms can be differentiated on the basis of the **intentions of the people** who are performing hacking activity. However, understanding the true intentions of hackers can be quite difficult.



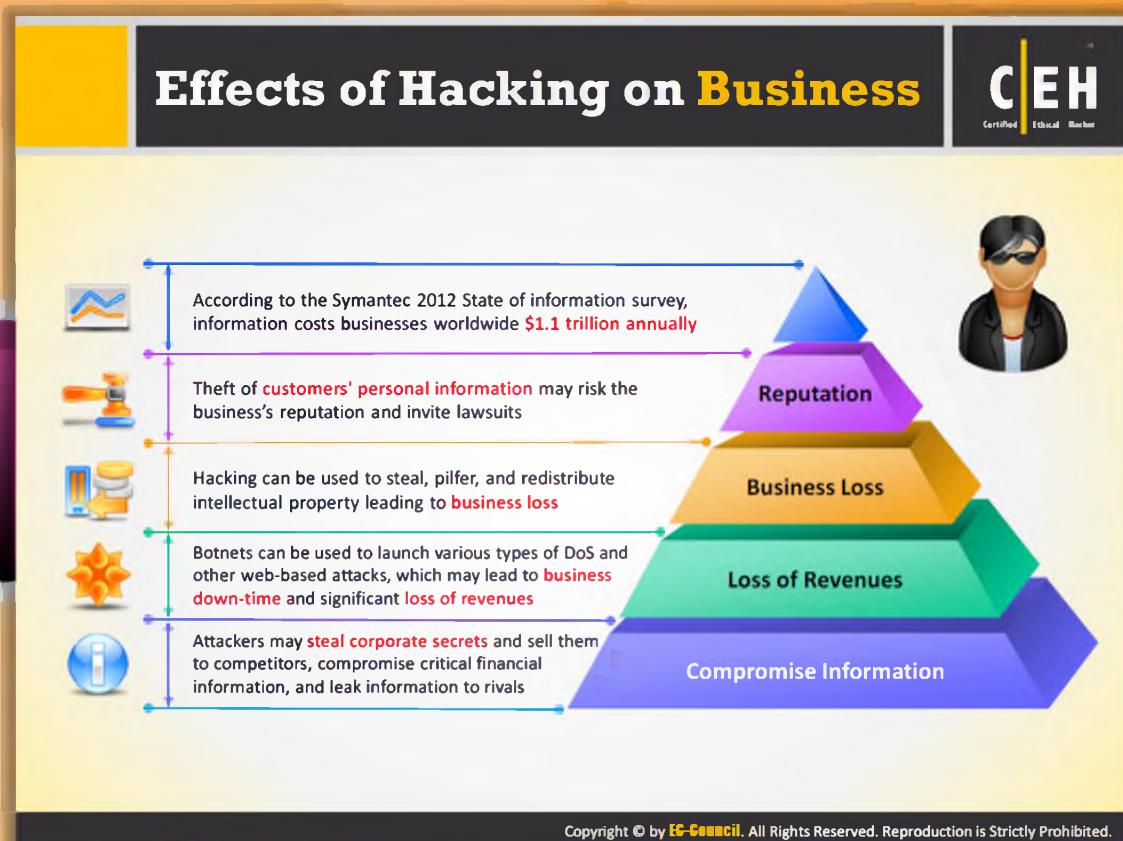
Hacking

Hacking refers to exploiting system vulnerabilities and **compromising security controls** to gain **unauthorized** or inappropriate **access** to the system resources. It involves modifying system or application features to achieve a goal outside of the creator's original purpose.



Ethical Hacking

Ethical hacking involves the use of **hacking tools**, tricks, and techniques to **identify vulnerabilities** so as to ensure system security. It focuses on simulating techniques used by attackers to verify the existence of exploitable vulnerabilities in the **system security**.



Effects of Hacking on Business

According to the Symantec 2012 State of Information survey, information costs businesses worldwide **\$1.1 trillion annually**. Every business must provide **strong security** for its customers; otherwise the business may put its reputation at stake and may even face lawsuits. Attackers use **hacking techniques** to steal, pilfer, and redistribute intellectual property of businesses and in turn to make financial gain. Attackers may profit, but the victim's business must face **huge financial losses** and may even lose its reputation.

Once an attacker gains control over the user's system, he or she can access all the files that are stored on the computer, including personal or corporate financial information, credit card numbers, and client or customer data stored on that system. If any such information falls into the wrong hands, it may create chaos in the normal functioning of an organization. Organizations must provide a strong security to its critical information sources containing customer data and its upcoming releases or ideas. If the data is altered or stolen, a company may lose credibility and the trust of its customers. In addition to the potential financial loss that may occur, the loss of information may cause a business to lose a crucial competitive advantage over its rivals. Sometimes attackers use **botnets** to launch various types of **DoS** and other **web-based attacks**. This causes the target business services to go down, which in turn may lead to loss of revenues.

There are many things that businesses can do to protect themselves and their assets. Knowledge is a key component in addressing this issue. Assessment of the risk prevalent in a business and how attacks could potentially affect that business is paramount from a security point of view. One does not have to be a security expert to recognize the damage that can occur when a company is victimized by an attacker. By understanding the problem and empowering employees to facilitate **protection** against attacks, the company would be able to deal with any **security issues** as they arise.

Who Is a Hacker?

C|EH
Certified Ethical Hacker

Excellent Computer Skills
Intelligent individuals with excellent computer skills, with the ability to create and explore into the computer's software and hardware

Hobby
For some hackers, hacking is a hobby to see how many computers or networks they can compromise

Do Illegal Things
Their intention can either be to gain knowledge or to poke around to do illegal things

Malicious Intent
Some do hacking with malicious intent behind their escapades, like stealing business data, credit card information, social security numbers, email passwords, etc.

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



Who Is a Hacker?

A hacker is a person who **illegally breaks** into a **system** or **network** without any authorization to destroy, steal sensitive data, or perform malicious attacks. Hackers may be motivated by a multitude of **reasons**:

- ➊ Intelligent individuals with excellent computer skills, with the ability to create and explore the computer's software and hardware
- ➋ For some hackers, hacking is a **hobby** to see how many computers or networks they can compromise
- ➌ Their intention can either be to **gain knowledge** or to **poke** around doing illegal things
- ➍ Some hack with malicious intent, such as **stealing business data**, **credit card information**, **social security numbers**, email **passwords**, etc.

Hacker Classes



Black Hats
Individuals with extraordinary computing skills, resorting to malicious or destructive activities and are also known as crackers

White Hats
Individuals professing hacker skills and using them for defensive purposes and are also known as security analysts

Gray Hats
Individuals who work both offensively and defensively at various times

Suicide Hackers
Individuals who aim to bring down critical infrastructure for a "cause" and are not worried about facing jail terms or any other kind of punishment

Script Kiddies
An unskilled hacker who compromises system by running scripts, tools, and software developed by real hackers

Spy Hackers
Individuals employed by the organization to penetrate and gain trade secrets of the competitor

Cyber Terrorists
Individuals with wide range of skills, motivated by religious or political beliefs to create fear by large-scale disruption of computer networks

State Sponsored Hackers
Individuals employed by the government to penetrate and gain top-secret information and to damage information systems of other governments

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

Hacker Classes

Hackers are mainly divided into eight classes:



Black Hats

Black hats are individuals with **extraordinary computing skills**, resorting to malicious or destructive activities and are also known as crackers. These individuals mostly use their skills for only destructive activities, causing huge losses for companies as well as individuals. They use their skills in finding vulnerabilities in the various networks including defense and government websites, banking and finance, etc. Some do it to cause damage, steal information, destroy data, or earn money easily by **hacking IDs** of bank customers.



White Hats

White hats are individuals who possess hacking skills and use them for defensive purposes; they are also known as **security analysts**. These days, almost every company has security analysts to defend their systems against the malicious attacks. White hats help companies secure their networks from outside intruders.



Gray Hats

Gray hats are the individuals who work both **offensively** and **defensively** at various times. Gray hats fall between white and black hats. Gray hats might help hackers by finding various vulnerabilities of a system or network and at the same time help vendors to improve products (software or hardware) by checking limitations and making them more secure, etc.



Suicide Hackers

Suicide hackers are individuals who aim to bring down critical infrastructure for a "**cause**" and are not worried about facing 30 years in jail for their actions. Suicide hackers are closely related to suicide bombers, who sacrifice their life for the attack and are not concerned with the consequences of their actions. There has been a rise in cyber terrorism in recent years.



Script Kiddies

Script kiddies are the **unskilled hackers** who compromise systems by running scripts, tools, and software developed by real hackers. They utilize small, **easy-to-use programs** or scripts as well as distinguished techniques to find and exploit the vulnerabilities of a machine. Script kiddies usually focus on the quantity of attacks rather than the quality of the attacks that they initiate.



Spy Hackers

Spy hackers are individuals who are employed by an organization to penetrate and gain trade secrets of the competitor. These insiders can take advantage of the privileges they have to hack a **system or network**.



Cyber Terrorists

Cyber terrorists could be **people, organized groups** formed by terrorist organizations, that have a wide range of skills, motivated by religious or political beliefs, to create fear by **large-scale disruption of computer networks**. This type of hacker is more dangerous as they can hack not only a website but whole Internet zones.



State Sponsored Hackers

State sponsored hackers are individuals employed by the government to penetrate and gain top-secret information and to **damage information systems** of other governments.

Hacktivism

C|EH
Certified Ethical Hacker

Hacktivism is an act of **promoting a political agenda** by hacking, especially by defacing or disabling websites

It **thrives in the environment** where information is easily accessible

Aims at **sending a message** through their hacking activities and gaining visibility for their cause

Common targets include **government agencies**, **multinational corporations**, or any other entity perceived as bad or wrong by these groups or individuals

It remains a fact, however, that **gaining unauthorized access** is a crime, no matter what the intention is

Hacktivism is motivated by revenge, political or social reasons, ideology, vandalism, protest, and a desire to **humiliate victims**

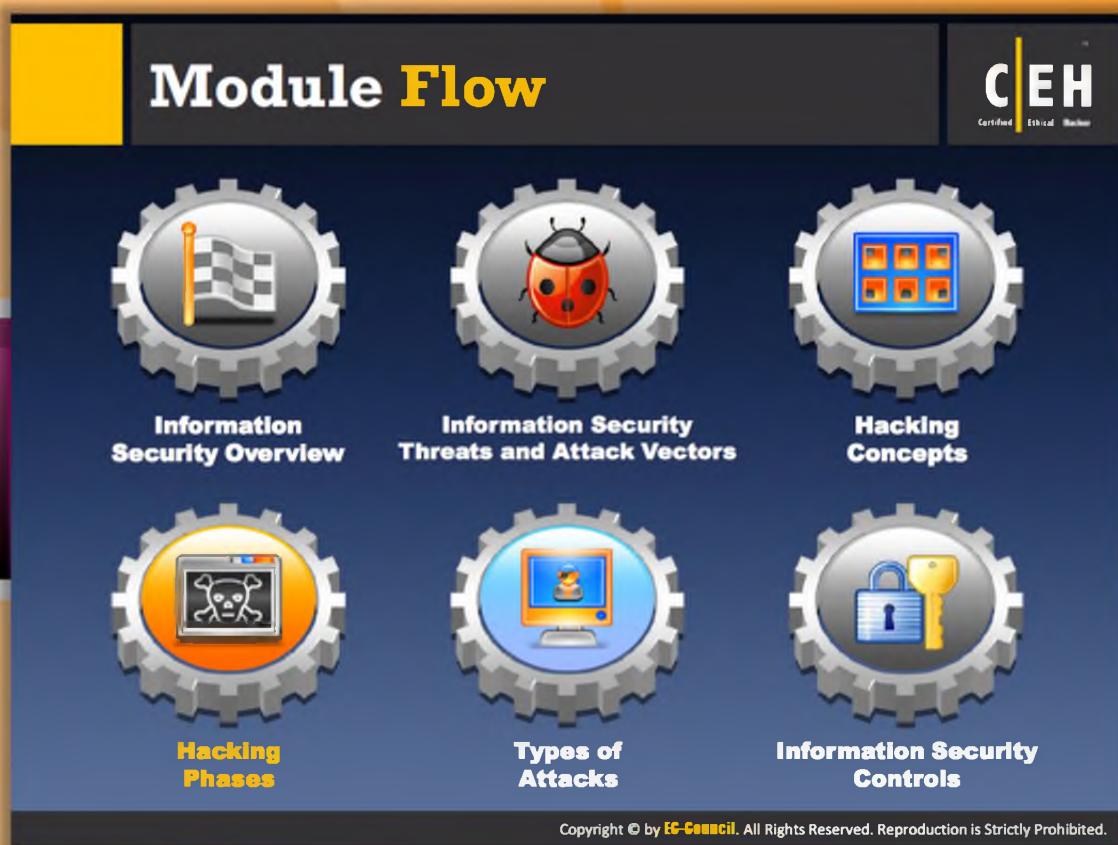
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



Hacktivism

Hacktivism is an act of promoting a **political agenda** by **hacking**, especially by defacing or disabling websites. The person who does these things is known as a hacktivist.

- ➊ Hacktivism thrives in an environment where information is **easily accessible**
- ➋ It aims to send a message through hacking activities and gain visibility for a cause.
- ➌ Common targets include government agencies, multinational corporations, or any other entity perceived as “**bad**” or “**wrong**” by these groups or individuals.
- ➍ It remains a fact, however, that gaining **unauthorized access** is a crime, no matter what the intention is.
- ➎ **Hacktivism** is motivated by revenge, **political** or **social** reasons, **ideology**, **vandalism**, protest, and a desire to humiliate victims.



Module Flow

In the previous section, you learned about various hacking concepts. Now it's time to discuss the **hacking method**. Hacking cannot be accomplished in a single action. It needs to be done in phases. The information gathered or the privileges gained in one phase can be used in the next phase for advancing the process of hacking.

 Information Security Overview	 Hacking Phases
 Information Security Threats and Attack Vectors	 Types of Attacks
 Hacking Concepts	 Information Security Controls

This section lists and describes various phases involved in hacking.

Hacking Phases

C|EH
Certified Ethical Hacker

The diagram illustrates the six phases of hacking as a vertical stack of colored circles. From top to bottom, the phases are: Reconnaissance (green), Scanning (light blue), Gaining Access (medium blue), Maintaining Access (dark blue), and Clearing Tracks (light green). Each phase is accompanied by a small icon: a magnifying glass for Reconnaissance, a network tower for Scanning, a key for Gaining Access, a shield for Maintaining Access, and a checkmark for Clearing Tracks.

Reconnaissance

- Reconnaissance refers to the preparatory phase where an **attacker** **seeks to gather information** about a target prior to launching an attack
- Could be the future point of return, noted for ease of entry for an attack when more about the **target is known on a broad scale**
- Reconnaissance **target range** may include the target organization's clients, employees, operations, network, and systems

Reconnaissance Types

Passive Reconnaissance

- Passive reconnaissance involves acquiring information without directly interacting with the target
- For example, searching public records or news releases

Active Reconnaissance

- Active reconnaissance involves interacting with the target directly by any means
- For example, telephone calls to the help desk or technical department

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



Hacking Phases

The various phases involved in hacking are:

- Reconnaissance
- Scanning
- Gaining Access
- Maintaining Access
- Clearing Tracks



Reconnaissance

Reconnaissance refers to the preparatory phase where an attacker **gathers** as much **information** as possible about the target prior to launching the attack. Also in this phase, the attacker draws on competitive intelligence to learn more about the target. This phase may also involve network scanning, either external or internal, without authorization.

This is the phase that allows the **potential attacker** to strategize his or her attack. This may take some time as the attacker waits to unearth crucial information. Part of this reconnaissance may

involve “**social engineering**.” A social engineer is a person who smooth-talks people into revealing information such as unlisted phone numbers, passwords, and other sensitive data.

Another reconnaissance technique is “**dumpster diving**.” Dumpster diving is the process of looking through an organization’s trash for discarded sensitive information. Attackers can use the Internet to obtain information such as employee’s contact information, business partners, technologies in use, and other critical business knowledge, but “dumpster diving” may provide them with even more sensitive information such as usernames, passwords, credit card statements, bank statements, ATM slips, social security numbers, telephone numbers, and so on. The reconnaissance target range may include the target organization’s clients, employees, operations, networks, and systems.

For example, a **Whois database** can provide information about Internet addresses, domain names, and contacts. If a potential attacker obtains **DNS information** from the registrar, and is able to access it, he or she can obtain useful information such as the mapping of domain names to IP addresses, mail servers, and host information records. It is important that a company has appropriate policies to protect its information assets, and also provide guidelines to its users of the same. Building user awareness of the precautions they must take in order to protect their information assets is a critical factor in this context.



Reconnaissance Types

Reconnaissance techniques can be categorized broadly into active and passive reconnaissance.

When an attacker approaches the attack using **passive reconnaissance** techniques, he or she does not interact with the system directly. The attacker uses publicly available information, social engineering, and dumpster diving as a means of gathering information.

When an attacker employs active reconnaissance techniques, he or she tries to interact with the system by using tools to detect open ports, accessible hosts, router locations, network mapping, details of operating systems, and applications.

The next phase of **attacking is scanning**, which is discussed in the following section. Some experts do not differentiate scanning from active reconnaissance. However, there is a slight difference as scanning involves more in-depth probing on the part of the attacker. Often reconnaissance and scanning phases overlap, and it is not always possible to demarcate these phases as watertight compartments.

Active reconnaissance is usually employed when the attacker discerns that there is a low probability that these reconnaissance activities will be detected. Newbies and script kiddies are often found attempting this to get faster, visible results, and sometimes just for the brag value they can obtain.

As an ethical hacker, you must be able to distinguish among the various reconnaissance methods, and be able to advocate preventive measures in the light of potential threats. Companies, for their part, must address security as an integral part of their business and/or operational strategy, and be equipped with **proper policies** and procedures to check for such activities.

Hacking Phases (Cont'd)



The diagram illustrates the five phases of hacking: Reconnaissance, Scanning, Gaining Access, Maintaining Access, and Clearing Tracks. The 'Scanning' phase is highlighted in orange. To the right, three specific attack methods are detailed: Pre-Attack Phase (Scanning), Port Scanner (Scanning), and Extract Information (Attacking). A sidebar provides a brief description of each.

Phase	Description
Reconnaissance	Gathering information about the target network.
Scanning	Identifying active hosts and open ports on the network.
Gaining Access	Obtaining user credentials or system access.
Maintaining Access	Keeping persistent access to the system.
Clearing Tracks	Erasing evidence of the attacker's presence.

Pre-Attack Phase
Scanning refers to the pre-attack phase when the attacker **scans the network** for specific information on the basis of information gathered during reconnaissance

Port Scanner
Scanning can include use of dialers, **port scanners**, network mappers, ping tools, vulnerability scanners, etc.

Extract Information
Attackers extract information such as **live machines**, port, port status, OS details, device type, **system uptime**, etc. to launch attack

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

Hacking Phases (Cont'd)



Scanning

Scanning is what an attacker does prior to **attacking the network**. In scanning, the attacker uses the details gathered during reconnaissance to identify specific vulnerabilities. Scanning can be considered a logical extension (and overlap) of the active reconnaissance. Often attackers use automated tools such as **network/host scanners** and war dialers to locate systems and attempt to discover vulnerabilities.

An attacker can gather critical network information such as the mapping of systems, routers, and firewalls by using simple tools such as **Traceroute**. Alternatively, they can use tools such as Cheops to add sweeping functionality along with what Traceroute renders.

Port scanners can be used to detect listening ports to find information about the nature of services running on the target machine. The primary defense technique in this regard is to shut down services that are not required. Appropriate filtering may also be adopted as a defense mechanism. However, attackers can still use tools to determine the rules implemented for filtering.

The most commonly used tools are vulnerability scanners that can search for several known vulnerabilities on a target network, and can potentially detect thousands of vulnerabilities. This gives the attacker the advantage of time because he or she only has to find a single means of

entry while the systems professional has to secure many vulnerable areas by applying patches. Organizations that deploy **intrusion detection systems (IDSe)** still have reason to worry because attackers can use evasion techniques at both the application and network levels.

Hacking Phases (Cont'd)

C|EH
Certified Ethical Hacker

The diagram illustrates the five phases of hacking:

- I**: Gaining access refers to the point where the attacker obtains access to the operating system or applications on the computer or network. (Icon: Person)
- II**: The attacker can gain access at the operating system level, application level, or network level. (Icon: Computer icons)
- III**: The attacker can escalate privileges to obtain complete control of the system. In the process, intermediate systems that are connected to it are also compromised. (Icon: Folders)
- IV**: Examples include password cracking, buffer overflows, denial of service, session hijacking, etc. (Icon: Bug)

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

Hacking Phases (Cont'd)



Gaining Access

Gaining access is the most important phase of an attack in terms of **potential damage**. Gaining access refers to the point where the attacker obtains access to the operating system or applications on the computer or network. The attacker can gain access at the operating system level, application level, or network level. Factors that influence the chances of an attacker gaining access into a target system include the **architecture** and **configuration** of the target system, the skill level of the perpetrator, and the initial level of access obtained. The attacker initially tries to gain minimal access to the target system or network. Once he or she gains the access, he or she tries to escalate privileges to obtain complete control of the system. In the process, intermediate systems that are connected to it are also compromised.

Attackers need not always gain access to the system to cause damage. For instance, denial-of-service attacks can either exhaust resources or stop services from running on the target system. Stopping of service can be carried out by killing processes, using a **logic/time bomb**, or even reconfiguring and crashing the system. Resources can be exhausted locally by filling up outgoing communication links.

The exploit can occur locally, offline, over a **LAN** or the **Internet** as a deception or theft. Examples include stack-based buffer overflows, denial-of-service, and session hijacking.

Attackers use a technique called spoofing to exploit the system by pretending to be strangers or different systems. They can use this technique to send a malformed packet containing a bug to the target system in order to exploit vulnerability. Packet flooding may be used to remotely stop availability of the essential services. **Smurf attacks** try to elicit a response from the available users on a network and then use their legitimate address to flood the victim.

Hacking Phases (Cont'd)

C|EH
Certified Ethical Hacker

The diagram features a vertical stack of five circles, each containing a phase name. From top to bottom, the circles are: 'Reconnaisance' (yellow), 'Scanning' (light blue), 'Gaining Access' (medium blue), 'Maintaining Access' (dark blue), and 'Clearing Tracks' (light grey). To the left of the circles is a vertical decorative element consisting of overlapping curved bands in yellow, light blue, and medium blue.

Maintaining access refers to the phase when the attacker tries to retain his or her ownership of the system	
Attackers may prevent the system from being owned by other attackers by securing their exclusive access with Backdoors, RootKits, or Trojans	
Attackers can upload, download, or manipulate data, applications, and configurations on the owned system	
Attackers use the compromised system to launch further attacks	

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

Hacking Phases (Cont'd)



Maintaining Access

Once an attacker gains access to the **target system**, the attacker can choose to use both the system and its resources and further use the system as a launch pad to scan and exploit other systems, or to keep a low profile and continue exploiting the system. Both these actions can damage the organization. For instance, the attacker can implement a sniffer to capture all network traffic, including telnet and ftp sessions with other systems.

Attackers, who choose to remain **undetected**, remove evidence of their entry and use a backdoor or a Trojan to gain repeat access. They can also install rootkits at the kernel level to gain super user access. The reason behind this is that rootkits gain access at the operating system level while a **Trojan horse** gains access at the application level. Both rootkits and Trojans depend on users to install them. Within **Windows systems**, most Trojans install themselves as a service and run as local system, which has administrative access.

Attackers can use **Trojan horses** to transfer **user names**, **passwords**, and even **credit card information** stored on the system. They can maintain control over their system for a long time by “**hardening**” the system against other attackers, and sometimes, in the process, do render some degree of protection to the system from other attacks. They can then use their access to steal data, consume CPU cycles, and trade sensitive information or even resort to extortion.

Organizations can use **intrusion detection systems** or deploy **honeypots** and **honeynets** to detect intruders. The latter though is not recommended unless the organization has the required security professional to leverage the concept for protection.



Hacking Phases (Cont'd)



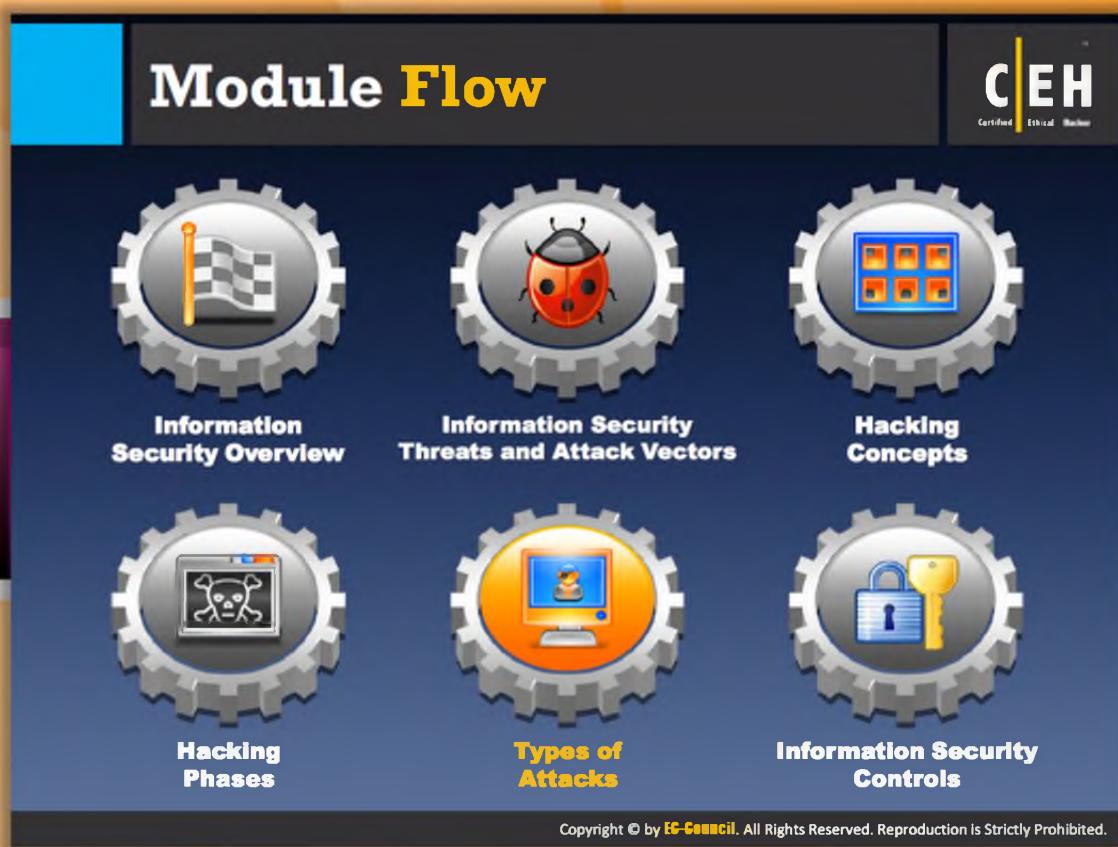
Clearing Tracks

An attacker would like to **destroy evidence** of his or her presence and activities for various reasons such as maintaining access and evading punitive action. **Trojans** such as **ps** or **netcat** come in handy for any attacker who wants to destroy the evidence from the log files or replace the system binaries with the same. Once the **Trojans** are in place, the attacker can be assumed to have gained total control of the system. Rootkits are automated tools that are designed to hide the presence of the attacker. By executing the script, a variety of critical files are replaced with Trojanized versions, **hiding** the **attacker** in seconds.

Other techniques include steganography and tunneling. **Steganography** is the process of hiding the data, for instance in images and sound files. Tunneling takes advantage of the transmission protocol by carrying one protocol over another. Even the extra space (e.g., unused bits) in the TCP and IP headers can be used for hiding information. An attacker can use the system as a cover to launch fresh attacks against other systems or use it as a means of reaching another system on the network **without** being detected. Thus, this phase of attack can turn into a new **cycle of attack** by using reconnaissance techniques all over again.

There have been instances where an attacker has lurked on a system even as system administrators have changed. The system administration can deploy **host-based IDSes** and anti-

virus tools that can detect Trojans and other seemingly benign files and directories. As an ethical hacker, you must be aware of the tools and techniques that attackers deploy, so that you are able to advocate and take **countermeasures** to ensure protection. These will be detailed in subsequent modules.



Module Flow

So far we discussed how important it is for an organization to keep their information resources secure, various security threats and attack vectors, hacking concepts, and the hacking phases. Now it's time to examine the **techniques** or the **type of attacks** the attacker adopts to hack a system or a network.

 Information Security Overview	 Hacking Phases
 Information Security Threats and Attack Vectors	 Types of Attacks
 Hacking Concepts	 Information Security Controls

This section covers various types of attacks such as **operating system attacks** and **application-level attacks**.

Types of Attacks on a System

C|EH
Certified Ethical Hacker

- Attackers exploit vulnerabilities in an information system to gain unauthorized access to the system resources
- The unauthorized access may result in loss, damage or theft of sensitive information



Types of Attacks

- I Operating System Attacks
- II Misconfiguration Attacks
- III Application Level Attacks
- IV Shrink Wrap Code Attacks

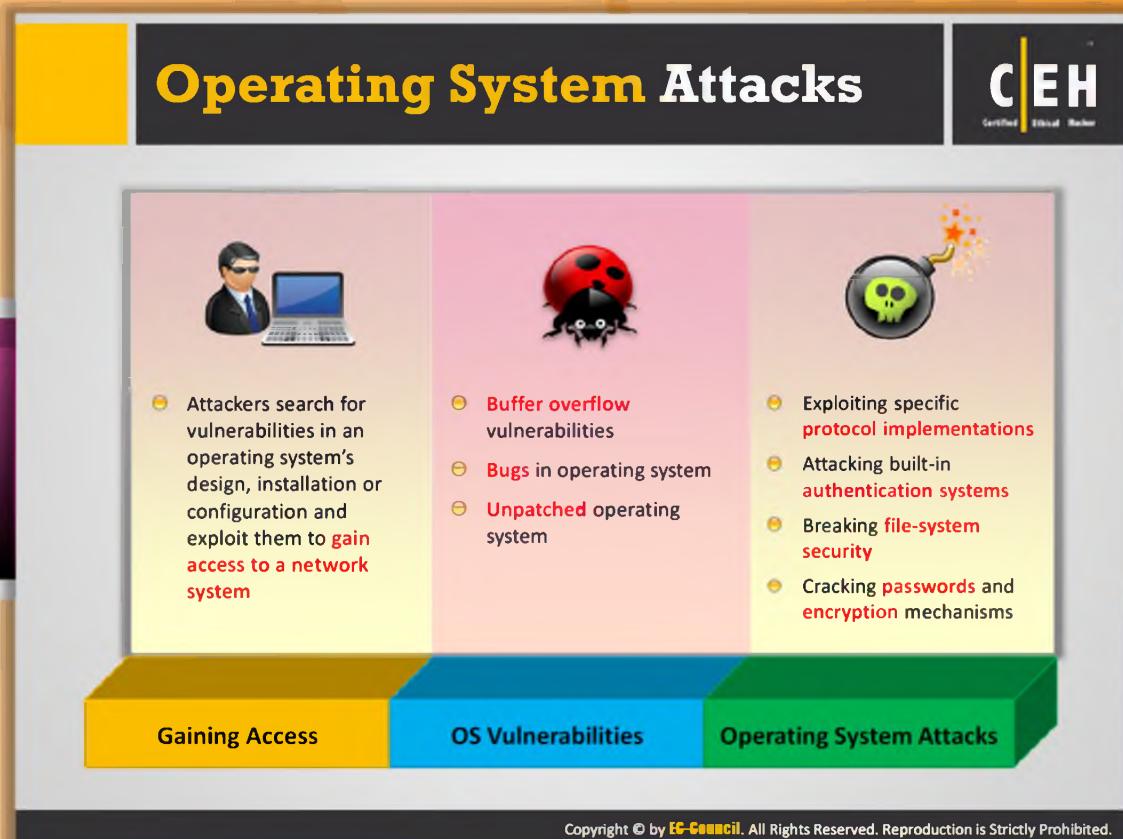
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



Types of Attacks on a System

There are several ways an attacker can gain access to a system. The attacker must be able to exploit a **weakness** or **vulnerability** in a system:

- **Operating system attacks:** Attackers search for **OS vulnerabilities** and exploit them to gain access to a network system.
- **Application-level attacks:** Software applications come with **myriad functionalities** and features. There is a dearth of time to perform complete testing before releasing products. Those applications have various vulnerabilities and become a source of attack.
- **Misconfiguration attacks:** Most administrators don't have the necessary skills to maintain or fix issues, which may lead to **configuration errors**. Such configuration errors may become the sources for an attacker to enter into the target's network or system.
- **Shrink wrap code attacks:** Operating system applications come with numerous **sample scripts** to make the job of administrator easy, but the same scripts have various vulnerabilities, which can lead to shrink wrap code attacks.



Operating System Attacks

Today's operating systems, which are loaded with features, are **increasingly complex**. While users take advantage of these features, the system is prone to more vulnerabilities, thus enticing attackers. Operating systems run many services such as **graphical user interfaces (GUIs)**. These supports the use of ports and modes of access to the Internet, and extensive tweaking is required to lock them down. Attackers are constantly looking for **OS vulnerabilities** so that they can exploit and gain access to network systems. To stop attackers from entering their network, the system or network administrators must keep abreast of various new exploits and methods adopted by attackers and monitor their **networks continuously**.

Most operating systems' installation programs install a large number of **services** and **open ports** by default. This situation leads attackers to search for various vulnerabilities. Applying **patches** and **hot fixes** is not easy with today's complex networks. Most patches and fixes tend to solve an immediate issue, but they cannot be considered a permanent solution.

Some OS vulnerabilities include:

- Buffer overflow vulnerabilities
- Bugs in the operating system
- Unpatched operating systems

Attacks performed at the OS level include:

- ➊ Exploiting specific **network protocol implementations**
- ➋ Attacking built-in authentication systems
- ➌ Breaking file system security
- ➍ Cracking **passwords** and **encryption mechanisms**

Misconfiguration Attacks

C|EH
Certified Ethical Hacker

If a system is **misconfigured**, such as a change is made in the file permission, it can no longer be considered **secure**

Misconfiguration vulnerabilities affect web servers, application platforms, databases, networks, or frameworks that may result in **illegal access** or possible owning of the system

The administrators are expected to **change the configuration of the devices** before they are deployed in the network. Failure to do this allows the default settings to be used to attack the system

In order to optimize the configuration of the machine, **remove any redundant services or software**

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



Misconfiguration Attacks

Misconfiguration vulnerabilities affect **web servers**, **application** platforms, **databases**, **networks**, or **frameworks** that may result in **illegal access** or possible owning of the system. If a system is misconfigured, such as when a change is made in the file permission, it can no longer be considered secure. Administrators are expected to change the configuration of the devices before they are deployed in the network. Failure to do this allows the default settings to be used to attack the system. In order to optimize the configuration of the machine, remove any redundant services or software.

Application-Level Attacks

C|EH
Certified Ethical Hacker

- Attackers exploit the vulnerabilities in applications running on organizations' information system to **gain unauthorized access** and **steal or manipulate data**

Poor or nonexistent error checking in applications leads to:

- Buffer overflow attacks
- Sensitive information disclosure
- Cross-site scripting
- Session hijacking and man-in-the-middle attacks
- Denial-of-service attacks
- SQL injection attacks

Other application-level attacks include:

- Phishing
- Session hijacking
- Man-in-the-middle attack
- Parameter/form tampering
- Directory traversal attacks

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



Application-level Attacks

Applications are being released with more features and more complex coding. With this increased demand in functionality and features, **developers generally overlook** the security of the application, which gives rise to vulnerabilities in applications. Attackers find and exploit these vulnerabilities in the applications using different tools and techniques. The applications are vulnerable to attack because of the following reasons:

- Software developers have **tight schedules to deliver** products on time
- Software applications come with a **multitude of features** and **functionalities**
- There is a **dearth of time to** perform complete **testing** before releasing products
- Security** is often an afterthought, and frequently delivered as an "**add-on**" component

Poor or nonexistent error checking in applications leads to:

- Buffer overflow attacks
- Active content
- Cross-site scripting
- Denial-of-service and SYN attacks

- ⌚ SQL injection attacks
- ⌚ Malicious bots

Other application-level attacks include:

- ⌚ Phishing
- ⌚ Session hijacking
- ⌚ Man-in-the-middle attacks
- ⌚ Parameter/form **tampering**
- ⌚ Directory traversal attacks

Examples of Application-Level Attacks

Session Hijacking

Vulnerable Code

```
1: <configuration>
2:   <system.web>
3:     <authentication mode="Forms">
4:       <forms cookieless="UseUri"> ...>
5:     </system.web>
6:   </configuration>
```

 Attacker may exploit session information in the vulnerable code to perform session hijacking

Secure Code

```
1: <configuration>
2:   <system.web>
3:     <authentication mode="Forms">
4:       <forms cookieless="UseCookies"> ...>
5:     </system.web>
6:   </configuration>
```

 The code can be secured by using **UseCookies** instead of **UseUri**

Denial-of-Service

Vulnerable Code

```
1: Statement stmt = conn.createStatement ();
2: ResultSet rsResultSet = stmt.executeQuery ();
3: stmt.close ();
```

 The code below is vulnerable to denial-of-service attack, as it fails to release connection resource

Secure Code

```
1: Statement stmt;
2: try {stmt = conn.createStatement ();
3: stmt.executeQuery ();
4: finally {
5: If (stmt!= null) {
6: try {stmt.close ();
7: } catch (SQLException sqlexp) { }
8: } catch (SQLException sqlexp) { }}
```

 The code can be secured by releasing the resources in a **finally** block

Note: For more information about application vulnerabilities and how to fix them attend EC-Council's ECSP program

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

Examples of Application-Level Attacks



Session Hijacking

Attackers may exploit session information in the vulnerable code to perform session hijacking when you enable **cookieless authentication** in your application. When the target tries to browse through a URL, the session or authentication token appears in the request URL instead of the secure cookie, to give access to the **URL requested** by the target. Here, an attacker using his or her skills and monitoring tools can hijack the targets session and steal all sensitive information.

Vulnerable Code

Attackers may exploit session information in the vulnerable code to perform session hijacking.

```
1: <configuration>
2:   <system.web>
3:     <authentication mode="Forms">
4:       <forms cookieless="UseUri">
5:     </system.web>
6:   </configuration>
```

TABLE 1.1: Session Hijacking Vulnerable Code

Secure Code

The code can be secured by using UseCookies instead of UseUri.

```
1: <configuration>
2:   <system.web>
3:     <authentication mode="Forms">
4:       <forms cookieless="UseCookies">
5:     </system.web>
6:   </configuration>
```

TABLE 1.2: Session Hijacking Secure Code



Denial-of-Service

Vulnerable Code

The code that follows is vulnerable to a denial-of-service attack, as it fails to release a connection resource.

```
1: Statement stmt = conn.createStatement ();
2: ResultSet rsltset = stmt.executeQuery ();
3: stmt.close ();
```

TABLE 1.3: Denial-of-Service Vulnerable Code

Secure Code

The code can be secured by releasing the resources in a finally block.

```
1: Statement stmt;
2: try {stmt = conn.createStatement ();
3: stmt.executeQuery (); }
4: finally {
5: If (stmt! = null) {
6: try { stmt.close ();
7: } catch (SQLException sqlexp) { }
8: } catch (SQLException sqlexp) { }
```

TABLE 1.4: Denial-of-Service Secure Code

Shrink Wrap Code Attacks



- Why reinvent the wheel when you can buy off-the-shelf **libraries** and code?
 - When you install an **OS** or **application**, it comes with supporting sample scripts to perform various administration tasks
 - Application developers also use **off-the-shelf libraries** and code to reduce development time and cost
 - The problem is **not fine tuning** or customizing these scripts
 - **Shrink wrap code** or **default code** attack refers to attacks that exploit default configuration and settings of the off-the-shelf libraries and code

```

Private Function CleanUpLine(ByVal sLine As String) As String
    Dim iQuoteCount As Long
    Dim iLocat As Long
    Dim sChar As String
    Dim sPrevChar As String

    ' Starts with "Pm" if it is a comment
    sLine = Trim(sLine)
    If Left(sLine, 2) = "Pm" Then
        For i = 3 To Len(sLine)
            If sLine(i) = " " Then
                Exit Function
            End If
        Next i
        ' Starts with " " if it is a comment
        If Left(sLine, 1) = " " Then
            CleanUpLine = ""
            Exit Function
        End If
    End If

    ' Contains " " anywhere as a comment, so treat it as a comment or as the
    ' start of a string
    If InStr(sLine, " ") > 0 Then
        'If InStr(sLine, " ") > 0 Then
        'sBreaker = " "
        iQuoteCount = 0

        For i = 1 To Len(sLine)
            sChar = Mid(sLine, i, 1)

            ' If we found " " then an even number of " " characters in front
            ' means it is the start of a comment, and odd number means it is
            ' part of a string
            If sChar = " " Then
                If iQuoteCount Mod 2 = 0 Then
                    sLine = Trim(Left(sLine, i - 1))
                    Exit For
                End If
            ElseIf sChar = """ Then
                iQuoteCount = iQuoteCount + 1
            End If
        Next i
        sPrevChar = sChar
        iLocat = i
    End If

    CleanUpLine = sLine
End Function

```

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

Shrink Wrap Code Attacks

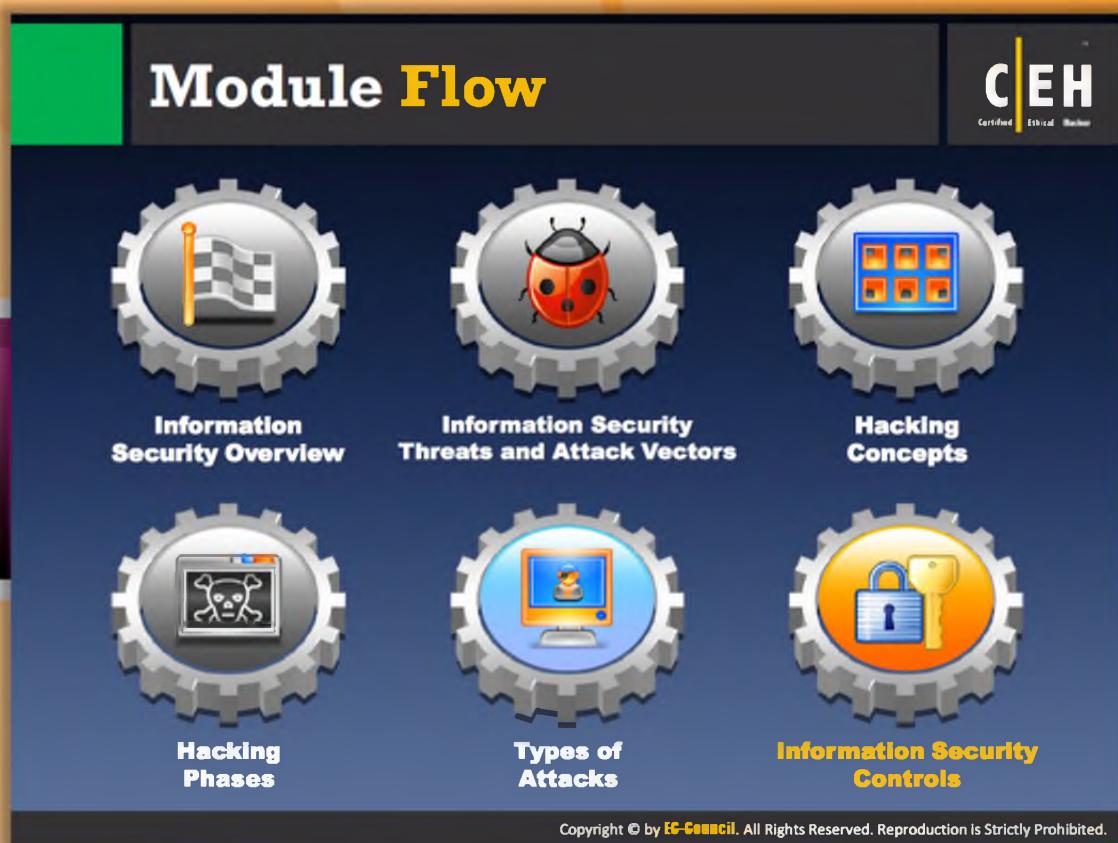
When you install an **OS/application**, it comes with many sample scripts to make the administrator's life easy.

- The problem is “**not fine tuning**” or customizing these scripts
 - This will lead to **default code** or **shrink wrap code attacks**

Code for shrink wraps code attacks

```
01522 Private Function ClearUpLine(ByVal sLine As String) As String
01523     Dim lQuoteCount As Long
01524     Dim lCount      As Long
01525     Dim sChar       As String
01526     Dim sPrevChar   As String
01527
01528     ' Starts with Rem it is a comment
01529     sLine = Trim(sLine)
01530     If Left(sLine, 3) = "Rem" Then
01531         ClearUpLine = ""
01532         Exit Function
01533     End If
01534
01535     ' Starts with ' it is a comment
01536     If Left(sLine, 1) = "'" Then
01537         ClearUpLine = ""
01538         Exit Function
01539     End If
01540
01541     ' Contains ' may end in a comment, so test if it is a comment or in the
01542     ' body of a string
01543     If InStr(sLine, "'") > 0 Then
01544         sPrevChar = " "
01545         lQuoteCount = 0
01546
01547     For lCount = 1 To Len(sLine)
01548         sChar = Mid(sLine, lCount, 1)
01549
01550         ' If we found " " then an even number of " characters in front
01551         ' means it is the start of a comment, and odd number means it is
01552         ' part of a string
01553         If sChar = " " And sPrevChar = " " Then
01554             If lQuoteCount Mod 2 = 0 Then
01555                 sLine = Trim(Left(sLine, lCount - 1))
01556                 Exit For
01557             End If
01558             ElseIf sChar = " " Then
01559                 lQuoteCount = lQuoteCount + 1
01560             End If
01561             sPrevChar = sChar
01562         Next lCount
01563     End If
01564
01565     ClearUpLine = sLine
01566 End Function
```

FIGURE 1.3: Shrink Wraps Code



Module flow

In the previous section, we discussed how an attacker can compromise an information system and what type of attacks an attacker can perform. Now, we will discuss **information security controls**. Information security controls **prevent unwanted events** from occurring and **reduces the risk** to the information assets of the organization with **security policies**.

Information Security Overview	Hacking Phases
Information Security Threats and Attack Vectors	Types of Attacks
Hacking Concepts	Information Security Controls

This section highlights the importance of ethical hacking and discusses various **security policies**.

Why Ethical Hacking is Necessary

To beat a hacker, you need to think like one!

Ethical hacking is necessary because it **allows the countering of attacks** from malicious hackers by anticipating methods they can use to break into a system



Reasons why Organizations Recruit Ethical Hackers

- To prevent hackers from gaining access to information breaches
- To fight against terrorism and national security breaches
- To build a system that avoids hackers from penetrating
- To test if organization's security settings are in fact secure



Ethical Hackers Try to Answer the Following Questions

- What can the intruder see on the **target system**? (Reconnaissance and Scanning phases)
- What can an **intruder do** with that information? (Gaining Access and Maintaining Access phases)
- Does anyone at the target **notice the intruders' attempts** or successes? (Reconnaissance and Covering Tracks phases)
- If all the **components of information system** are adequately protected, updated, and patched
- How much effort, time, and money is required to obtain **adequate protection**?
- Does the **information security measures** are in compliance to industry and legal standards?

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



Why Ethical Hacking Is Necessary

There is rapid growth in technology, so there is growth in the risks associated with the technology. **Ethical hacking** helps to **predict** the various possible **vulnerabilities** well in advance and rectify them without incurring any kind of attack from outsiders.

- **Ethical Hacking:** As hacking involves creative thinking, **vulnerability testing** and **security audits** cannot ensure that the network is secure.
- **Defense-in-Depth Strategy:** To achieve this, organizations need to implement a "**defense-in-depth**" strategy by penetrating their networks to **estimate vulnerabilities** and expose them.
- **Counter the Attacks:** Ethical hacking is necessary because it allows countering of attacks from malicious hackers by **anticipating methods** they can use to break into a system.

Scope and Limitations of Ethical Hacking

Scope

- Ethical hacking is a crucial component of risk assessment, auditing, counter fraud, best practices, and good governance
- It is used to identify risks and highlight the remedial actions, and also reduces information and communications technology (ICT) costs by resolving those vulnerabilities

Limitations

- However, unless the businesses first know what it is that they are looking for and why they are hiring an outside vendor to hack systems in the first place, chances are there would not be much to gain from the experience
- An ethical hacker thus can only help the organization to better understand their security system, but it is up to the organization to place the right guards on the network

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



Scope and Limitations of Ethical Hacking

Ethical hacking has a scope, and there are various limitations of ethical hacking, as well.



Scope

The following is the scope of ethical hacking:

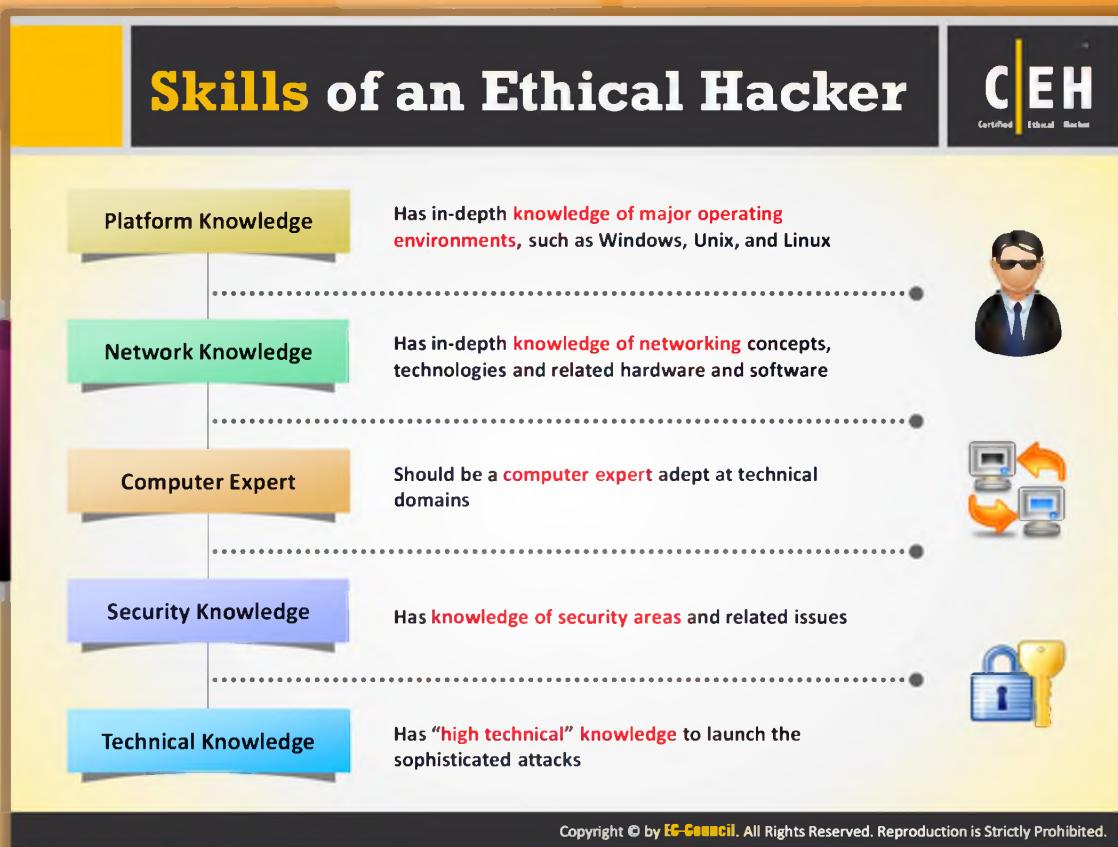
- Ethical hacking is a crucial component of risk assessment, auditing, counter fraud, best practices, and good governance.
- It is used to identify risks and highlight remedial actions, and it reduces information and communications technology (ICT) costs by resolving those vulnerabilities.



Limitations

The following are the limitations of ethical hacking:

- Unless businesses first know what it is they are looking for and why they are hiring an outside vendor to hack systems in the first place; chances are that there will not be much to gain from the experience.
- An ethical hacker therefore can help the organization only to better understand their security system, but it is up to the organization to implement the right safeguards on the network.

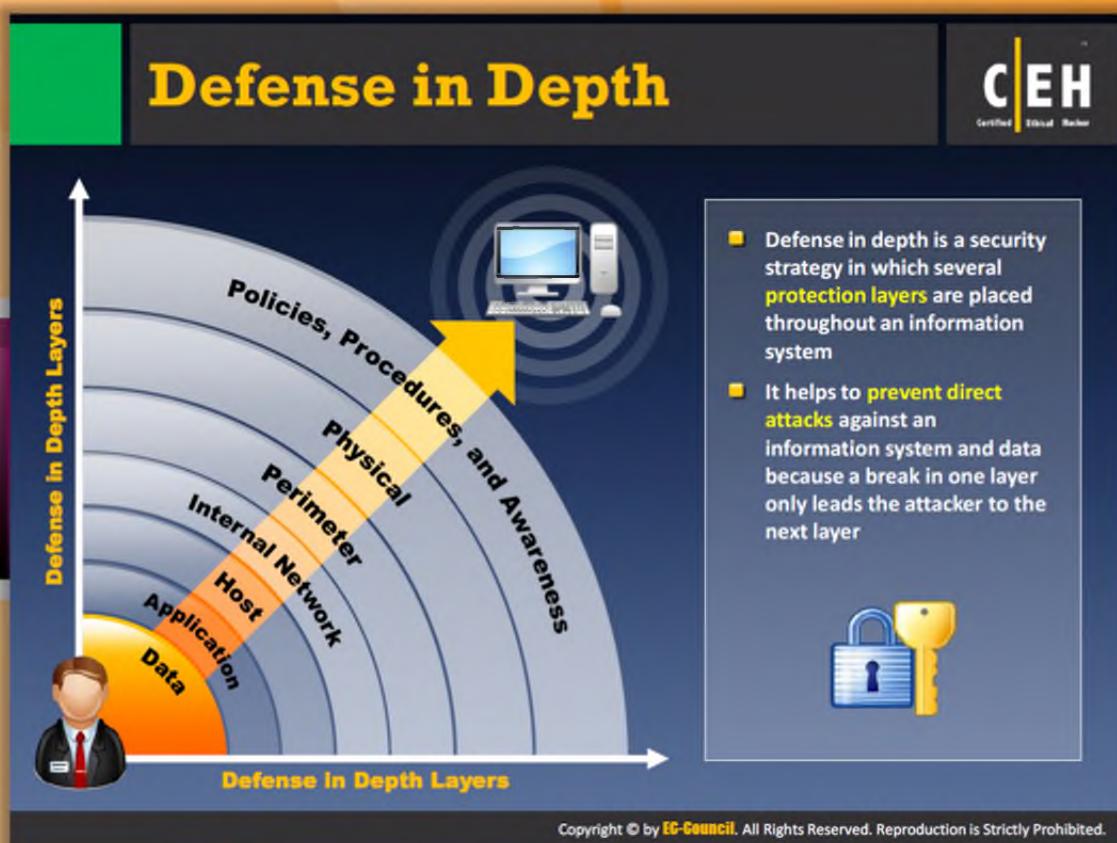


Skills of an Ethical Hacker

Ethical hacking is the **legal hacking** performed by pen tester to **find vulnerabilities** in the information technology environment. In order to perform ethical hacking, the ethical hacker requires the skills of a computer expert. Ethical hackers should also have strong computer knowledge including **programming** and **networking**. They should be proficient at installing and maintaining systems using popular operating systems (e.g. UNIX, Windows, or Linux).

Detailed knowledge of **hardware** and **software** provided by popular computer and networking hardware vendors complement this basic knowledge. It is not always necessary that ethical hackers possess any additional specialization in security. However, it is an advantage to know how various systems maintain their security. **Management skills** pertaining to these systems are necessary for actual vulnerability testing and for preparing the report after the testing is carried out.

An ethical hacker should possess immense patience as the analysis stage consumes more time than the testing stage. The **time frame** for an evaluation may **vary** from a few days to several weeks, depending on the nature of the task. When an ethical hacker encounters a system with which he or she is not familiar, it is imperative the person takes the time to learn everything about the system and try to find its **vulnerable spots**.



Defense-in-Depth

Multiple defense-in-depth countermeasures are taken to **protect information** assets of a company. The strategy is based on the military principle that it is more difficult for an enemy to defeat a complex and **multi-layered defense system** than to penetrate a single barrier. If a hacker gains access to a system, defense-in-depth minimizes the adverse impact and gives administrators and engineers time to deploy new or updated countermeasures to prevent a recurrence.

- ➊ Defense-in-depth is a security strategy in which **several protection layers** are placed throughout an information system.
- ➋ It helps to prevent direct attacks against an information system and data because a break in one layer only leads the attacker to the next layer.

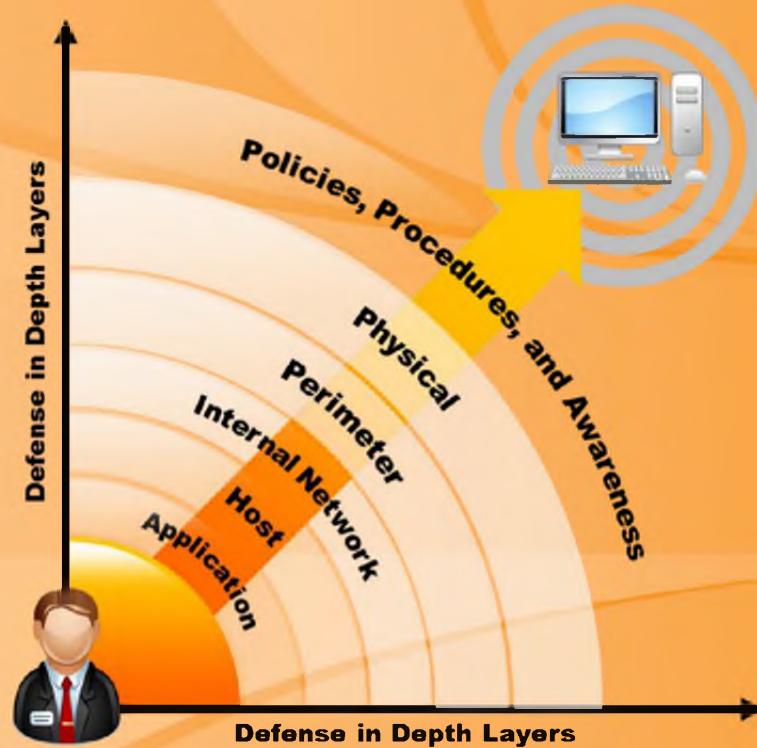


FIGURE 1.4: Defense in Depth Layers Diagram

Incident Management Process

C|EH
Certified Ethical Hacker

Incident management is a set of defined processes to **identify, analyze, prioritize, and resolve security incidents** to restore normal service operations as quickly as possible and prevent future reoccurrence of the incident

Purpose of incident management process

- 1 Improves service quality
- 2 Pro-active problem resolution
- 3 Reduces impact of incidents on business/organization
- 4 Meets service availability requirements
- 5 Increases staff efficiency and productivity
- 6 Improves user/customer satisfaction
- 7 Assists in handling future incidents

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

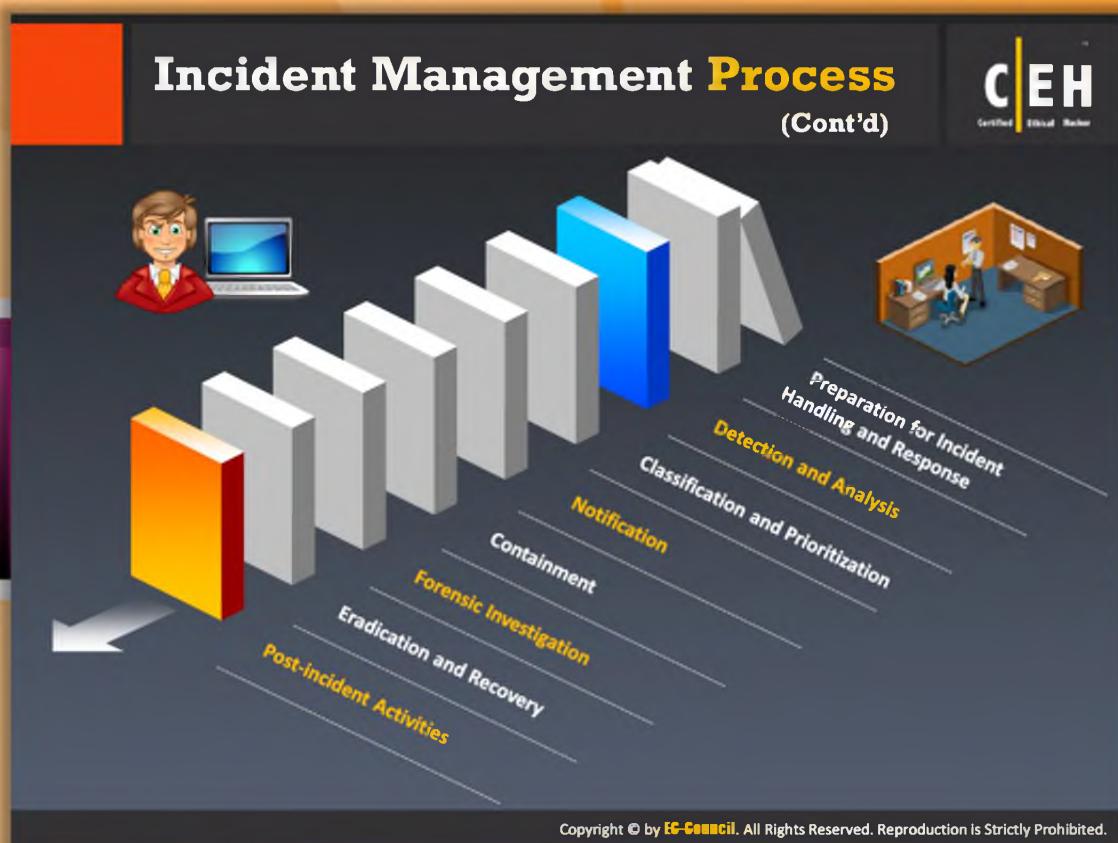


Incident Management Process

Incident management is a set of defined processes to identify, analyze, prioritize, and resolve security incidents to restore the system to normal service operations as soon as possible and prevent the recurrence of the same incident.

The purpose of the incident management process:

- ➊ Improves service quality
- ➋ Pro-active problem resolution
- ➌ Reduces impact of incidents on business/organization
- ➍ Meets service availability requirements
- ➎ Increases staff efficiency and productivity
- ➏ Improves user/customer satisfaction
- ➐ Assists in handling future incidents



Incident Management Process (Cont'd)

Incident management is the process of **logging**, **recording**, and **resolving** incidents that take place in the organization. The incident may occur due to fault, service degradation, error, etc. The incidents are reported by users, technical staff, or sometimes detected automatically by event **monitoring tools**. The main objective of the incident management process is to restore the service to a normal stage as early as possible to customers, while maintaining availability and quality of service. Any occurrence of the incident in an organization is handled and resolved by following these incident management steps:

- Preparation for Incident Handling and Response
- Detection and Analysis
- Classification and Prioritization
- Notification
- Containment
- Forensic Investigation
- Eradication and Recovery
- Post-incident Activities

Information Security Policies

C|EH
Certified Ethical Hacker

- Security policies are the foundation of the **security infrastructure**
- A security policy is a document or set of documents that **describes the security controls** that will be implemented in the company at a high level

Goals of Security Policies

1. Maintain an outline for the management and administration of network security	5. Prevent unauthorized modifications of the data
2. Protection of organization's computing resources	6. Reduce risks caused by illegal use of the system resource, loss of sensitive, confidential data, and potential property
3. Elimination of legal liability from employees or third parties	7. Differentiate the user's access rights
4. Ensure customers' integrity and prevent waste of company computing resources	9. Protect confidential, proprietary information from theft, misuse, unauthorized disclosure

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



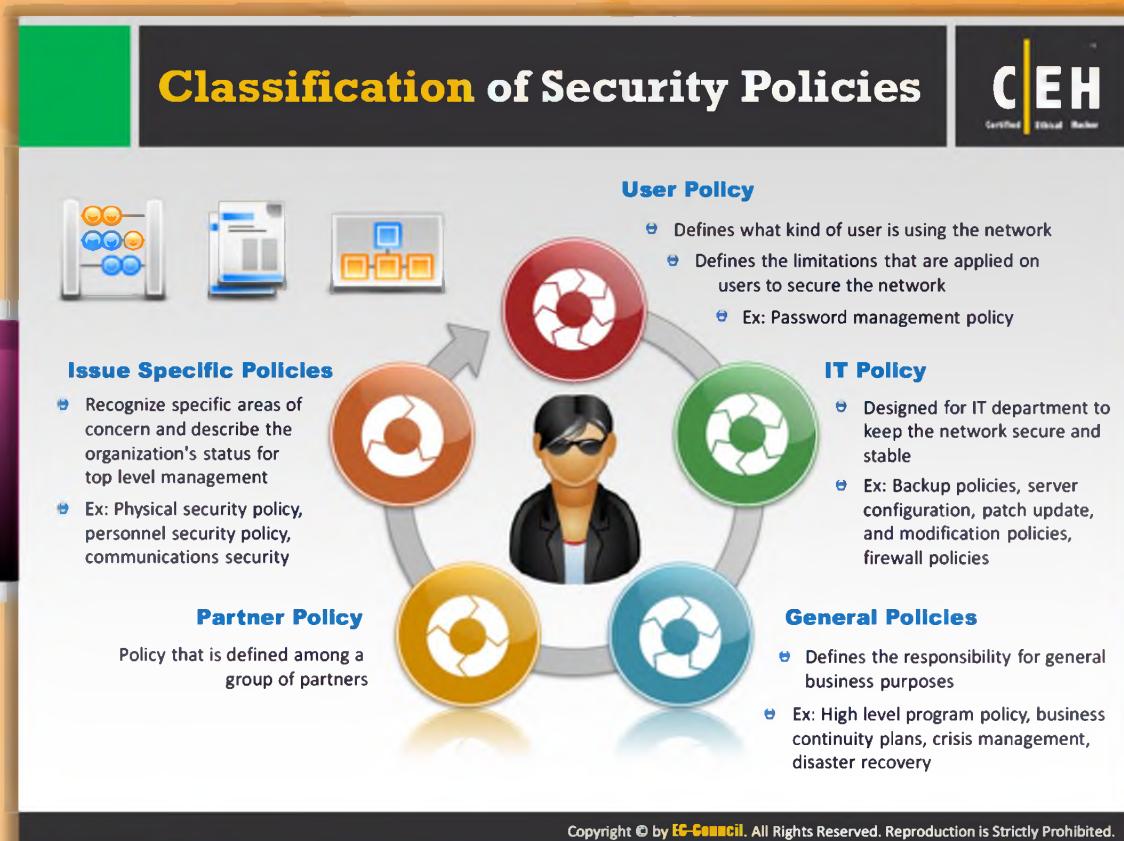
Information Security Policies

A security policy is a document or set of documents that describes the security controls that should be implemented in the company at a **high level for safeguarding** the organizational network from inside and outside attacks. This document defines the complete security architecture of an organization and the document includes clear objectives, goals, rules and regulations, formal procedures, and so on. It clearly mentions the assets to be protected and the person who can log in and access sites, who can view the selected data, as well as the people who are allowed to change the data, etc. Without these policies, it is impossible to protect the company from possible lawsuits, lost revenue, and so on.

Security policies are the foundation of the **security infrastructure**. These policies secure and safeguard the information resources of an organization and provide legal protection to the organization. These policies are beneficial since they help bring awareness of the staff working in the organization to work together to secure its communication, as well as minimizing the risks of security weaknesses through "**human-factor**" mistakes such as disclosing sensitive information to unauthorized or unknown sources, improper use of Internet, etc. In addition, these policies provide protection against cyber-attacks, malicious threats, foreign intelligence, and so on. They mainly address physical security, network security, access authorizations, virus protection, and disaster recovery.

The goals of security policies include:

- ⌚ Maintain an **outline** for the management and administration of network security
- ⌚ Protection of organization's computing resources
- ⌚ **Elimination of legal liability** from employees or third parties
- ⌚ Ensure customers' **integrity** and prevent wasting of company computing resources
- ⌚ **Prevent unauthorized modifications** of data
- ⌚ **Reduce risks** caused by illegal use of the system resources and loss of sensitive, confidential data and potential property
- ⌚ Differentiate a user's access rights
- ⌚ Protect confidential, proprietary information from theft, misuse, or **unauthorized disclosure**



Classification of Security Policies

Security policies are sets of policies that are developed to protect or safeguard a company's information assets, networks, etc. These policies are applicable to users, IT departments, organization, and so on. For effective security management, security policies are classified into five different areas:



User Policy

- Defines what kind of user is using the network
- Defines the limitations that are applied on users to secure the network
- Ex: Password Management Policy



IT Policy

Designed for an IT department to keep the network secure and stable

Ex: backup policies, server configuration, patch updates, modification policies, firewall policies



General Policies

Define the responsibility for general business purposes

Ex: high-level program policy, business continuity plans, crisis management, disaster recovery



Partner Policy

Policy that is defined among a group of partners



Issue-specific Policies

Recognize specific areas of concern and describe the organization's status for top-level management

Ex: physical security policy, personnel security policy, communications security

Structure and Contents of Security Policies



Security Policy Structure

- Detailed description of the policy issues
- Description about the status of the policy
- Applicability of the policy to the environment
- Functionalities of those affected by the policy
- Compatibility level of the policy is necessary
- End-consequences of non-compliance



Contents of Security Policies

- High-level security requirements: Requirement of a system to implement security policies
- Policy description: Focuses on security disciplines, safeguards, procedures, continuity of operations, and documentation
- Security concept of operation: Defines the roles, responsibilities, and functions of a security policy
- Allocation of security enforcement to architecture elements: Provides a computer system architecture allocation to each system of the program

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

Structure and Contents of Security Policies



Structure of Security Policies

A security policy is the document that provides the way of securing the company's physical personnel and data from threats or security breaches. Security policies should be structured very carefully and should be reviewed properly to make sure that there is no wording that someone could take advantage of. The basic structure of security policies should include the following:

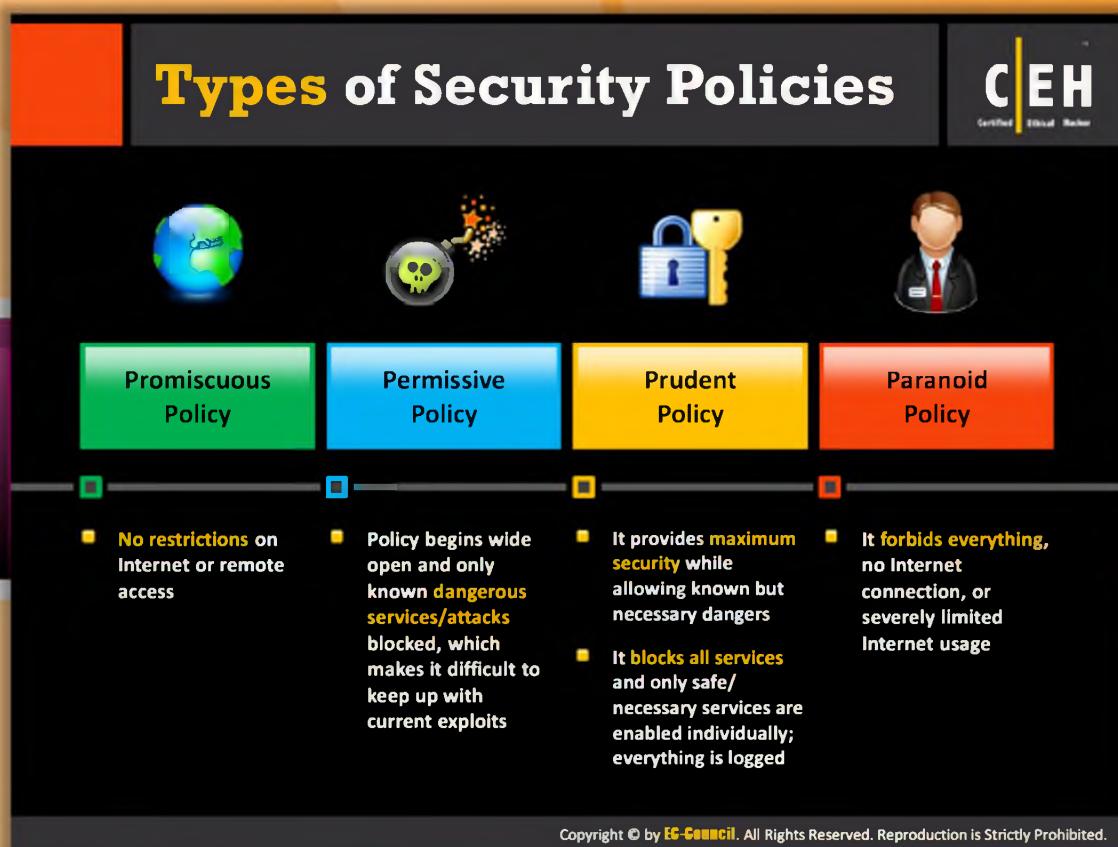
- Detailed description of the policy issues
- Description of the status of the policy
- Applicability of the policy to the environment
- Functionalities of those affected by the policy
- Specific consequences that will occur if the policy is not compatible with the organizational standards



Content of Security Policies

Security policies contain the following elements:

- ➊ **High-level Security Requirements:** Explains the **requirements** of a system for the security policies to be implemented. The four different types of requirements are **discipline**, **safeguard**, **procedural**, and **assurance**.
- ➋ **Discipline Security Requirements:** This requirement includes various security policies such as **communications** security, **computer** security, **operations** security, **emanations** security, **network** security, **personnel** security, **information** security, and **physical security**.
- ➌ **Safeguard Security Requirements:** This requirement mainly contains access control, archive, audit, authenticity, **availability**, **confidentiality**, cryptography, identification and authentication, integrity, interfaces, marking, **non-repudiation**, object reuse, recovery, and **virus protection**.
- ➍ **Procedural Security Requirements:** This requirement mainly contains **access** policies, **accountability** rules, **continuity-of-operations** plans, and documentation.
- ➎ **Assurance Security:** This includes **certification** and **accreditation reviews** and sustaining planning documents used in the assurance process.
- ➏ **Policy Description:** Focuses on security disciplines, **safeguards**, procedures, continuity of operations, and documentation. Each subset of this portion of the policy describes how the system's architecture will **enforce security**.
- ➐ **Security Concept of Operation:** Mainly defines the **roles**, **responsibilities**, and **functions** of a security policy. It focuses on mission, communications, encryption, user and maintenance rules, idle-time management, use of privately owned versus public-domain software, shareware software rules, and a virus protection policy.
- ➑ **Allocation of Security Enforcement to Architecture Elements:** Provides a computer system architecture allocation to each system of the program.



Types of Security Policies

A security policy is a **document** that **contains information** on the way the company plans to protect its **information assets** from **known** and **unknown threats**. These policies help to maintain the confidentiality, availability, and integrity of information. The four major types of security policies are as follows:



Promiscuous Policy

With a promiscuous policy, there is **no restriction on Internet access**. A user can access any site, download any application, and access a computer or a network from a remote location. While this can be useful in corporate businesses where people who travel or work at branch offices need to access the organizational networks, many malware, virus, and Trojan threats are present on the Internet. Due to free Internet access, this malware can come as attachments without the knowledge of the user. **Network administrators** must be extremely alert if this type of policy is chosen.



Permissive Policy

In a permissive policy, the majority of Internet traffic is accepted, but several known **dangerous services** and attacks are blocked. Because only known attacks and exploits are

blocked, it is impossible for administrators to keep up with current exploits. Administrators are always playing catch-up with new attacks and exploits.



Prudent Policy

A prudent policy starts with all **services blocked**. The administrator enables safe and necessary services individually. This provides **maximum security**. Everything, such as system and network activities, is logged.



Paranoid Policy

In a paranoid policy, everything is forbidden. There is **strict restriction** on all usage of company computers, whether it is **system usage** or **network usage**. There is either no Internet connection or severely limited Internet usage. Due to these overly severe restrictions, users often try to find ways around them.



Steps to Create and Implement Security Policies

Implementing **security policies reduces** the **risk** of being attacked. Thus, every company must have its own security policies based on its business. The following are the steps to be followed by every organization in order to create and implement security policies:

1. Perform **risk assessment** to identify risks to the organization's assets
2. Learn from **standard guidelines** and other organizations
3. Include **senior management** and all other staff in policy development
4. **Set clear penalties** and enforce them and also review and update the security policy
5. Make the final version available to all staff in the organization
6. Ensure every member of your staff reads, signs, and understands the policy
7. Install the tools you need to **enforce the policy**
8. **Train your employees** and educate them about the policy

Examples of Security Policies

C|EH
Certified Ethical Hacker

Acceptable-Use Policy	It defines the acceptable use of system resources
User-Account Policy	It defines the account creation process and authority, rights and responsibilities of user accounts
Remote-Access Policy	It defines who can have remote access, and defines access medium and remote access security controls
Information-Protection Policy	It defines the sensitivity levels of information , who may have access, how is it stored and transmitted, and how should it be deleted from storage media
Firewall-Management Policy	It defines access, management, and monitoring of firewalls in the organization
Special-Access Policy	This policy defines the terms and conditions of granting special access to system resources
Network-Connection Policy	It defines who can install new resources on the network , approve the installation of new devices, document network changes, etc.
Email Security Policy	It is created to govern the proper usage of corporate email
Passwords Policy	It provides guidelines for using strong password protection on organization's resources

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



Examples of Security Policies

The following are some examples of security policies that are created, accepted, and used by organizations worldwide to secure their assets and important resources.

Acceptable-Use Policy

Defines the acceptable use of **system resources**

User-Account Policy

Defines the account creation process and **authority, rights, and responsibilities** of user accounts

Remote-Access Policy

Defines who can have remote access, and **defines access medium** and remote access security controls

Information-Protection Policy

Defines the **sensitivity levels** of information, who may have access, how is it stored and transmitted, and how should it be deleted from storage media

Firewall-Management Policy

Defines **access, management**, and **monitoring** of firewalls in the organization

Special-Access Policy

This policy defines the **terms and conditions** of granting special access to system resources

Network-Connection Policy

Defines who can install **new resources** on the network, approve the installation of new devices, document network changes, etc.

Email Security Policy

Created to govern the proper **usage of corporate email**

Password Policy

Provides guidelines for using **strong password protection** on organization's resources

Vulnerability Research

The process of **discovering vulnerabilities and design flaws** that will open an operating system and its applications to attack or misuse

Vulnerabilities are classified based on **severity level** (low, medium, or high) and **exploit range** (local or remote)

An administrator needs vulnerability research:

- 1 To gather information about security trends, threats, and attacks
- 2 To find weaknesses and alert the network administrator before a network attack
- 3 To get information that helps to prevent the security problems
- 4 To know how to recover from a network attack

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



Vulnerability Research

Vulnerability research means **discovering system design faults** and weaknesses that might help attackers compromise the system. Once the attacker finds out the vulnerability in the product or the application, he or she tries to **exploit** it.

Vulnerability research helps both security administrators and attackers:

- Discovering system design faults and **weaknesses** that might help attackers to compromise the system
- Keeping abreast of the latest **vendor-supported products** and other technologies in order to find news related to current exploits
- **Checking** newly released **alerts** regarding relevant innovations and product improvements for security systems
- Vulnerability research is based on the following classification:
 - **Severity level** (low, medium, or high)
 - **Exploit range** (local or remote)

An administrator needs vulnerability research:

- To gather information about security trends, threats, and attacks
- To find weaknesses and alert the network administrator before a network attack
- To get information that helps to prevent security problems
- To know how **to recover** from a network attack

Vulnerability Research Websites

 CodeRed Center http://www.eccouncil.org	 HackerStorm http://www.hackerstorm.co.uk
 TechNet http://blogs.technet.com	 SC Magazine http://www.scmagazine.com
 Security Magazine http://www.securitymagazine.com	 Computerworld http://www.computerworld.com
 SecurityFocus http://www.securityfocus.com	 HackerJournals http://www.hackerjournals.com
 Help Net Security http://www.net-security.org	 WindowsSecurity Blogs http://blogs.windowsecurity.com

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



Vulnerability Research Websites

The following are the some vulnerability research websites that you can use:



CodeRed Center

Source: <http://www.eccouncil.org>

The CodeRed Center is a comprehensive **security resource administrators** can turn to for daily, accurate, up-to-date information on the latest viruses, Trojans, malware, threats, security tools, risks, and vulnerabilities.



TechNet

Source: <http://blogs.technet.com>

TechNet is a project team from across **Microsoft Lync Server** teams and the community at large. It is led by the Lync Server documentation team; their writers and technical reviewers come from all disciplines, including product engineers, field engineers, support engineers, documentation engineers, and some of the most respected technology bloggers and authors in the Lync Server universe.



Security Magazine

Source: <http://www.securitymagazine.com>

Security Magazine is uniquely focused on solutions for enterprise security leaders. It is designed and written for business-minded executives who manage **enterprise risk and security**. Security Magazine provides management-focused features, opinions, and trends for leaders in business.



SecurityFocus

Source: <http://www.securityfocus.com>

The Security Focus website focuses on a few key areas that are of greatest importance to the security community.

- ⦿ **BugTraq** is a high-volume, full-disclosure mailing list for the detailed discussion and announcement of computer security vulnerabilities. BugTraq serves as the cornerstone of the Internet-wide security community.
- ⦿ The **SecurityFocus Vulnerability Database** provides security professionals with the most up-to-date information on vulnerabilities for all platforms and services.



Help Net Security

Source: <http://www.net-security.org>

Net Security is a daily security news site that has been covering the latest computer and network security news since its inception in 1998.

Besides covering news around the globe, HNS focuses on quality technical articles and papers, vulnerabilities, vendor advisories, malware, and hosts the largest security software download area with software for Windows, Linux, and Mac OS X.



HackerStorm

Source: <http://www.hackerstorm.co.uk>

HackerStorm is a security resource for **ethical hackers** and **penetration testers** to create better penetration testing plans and scopes, and conduct vulnerability research.



SC Magazine

Source: <http://www.scmagazine.com>

SC Magazine is published by Haymarket Media Inc. and is part of a global brand. There are three separate editions of the magazine:

- ⦿ North America - U.S. and Canada
- ⦿ International - U.K. and mainland Europe

- ④ Asia Pacific Online - read by decision-makers in over **20 countries** in the Pacific Rim region

The magazine is published monthly, usually in the first week of each month. It is the longest running information security magazine in the world, with the widest distribution.

SC Magazine provides IT security professionals with in-depth and unbiased information in one incomparable publication. In each monthly issue it has timely news, comprehensive analysis, cutting-edge features, contributions from thought leaders and the best, most extensive collection of product reviews in the business. They have been doing this since 1989, when it first began campaigning for organizations' information security leaders, making it the longest established IT security title in the United States.



Computerworld

Source: <http://www.computerworld.com>

For more than **40 years**, Computerworld has been the leading source of technology news and information for IT influencers worldwide. **Computerworld's website** (Computerworld.com), twice-monthly publication, focused conference series, and custom research form the hub of the world's largest global IT media network.



HackerJournals

Source: <http://www.hackerjournals.com>

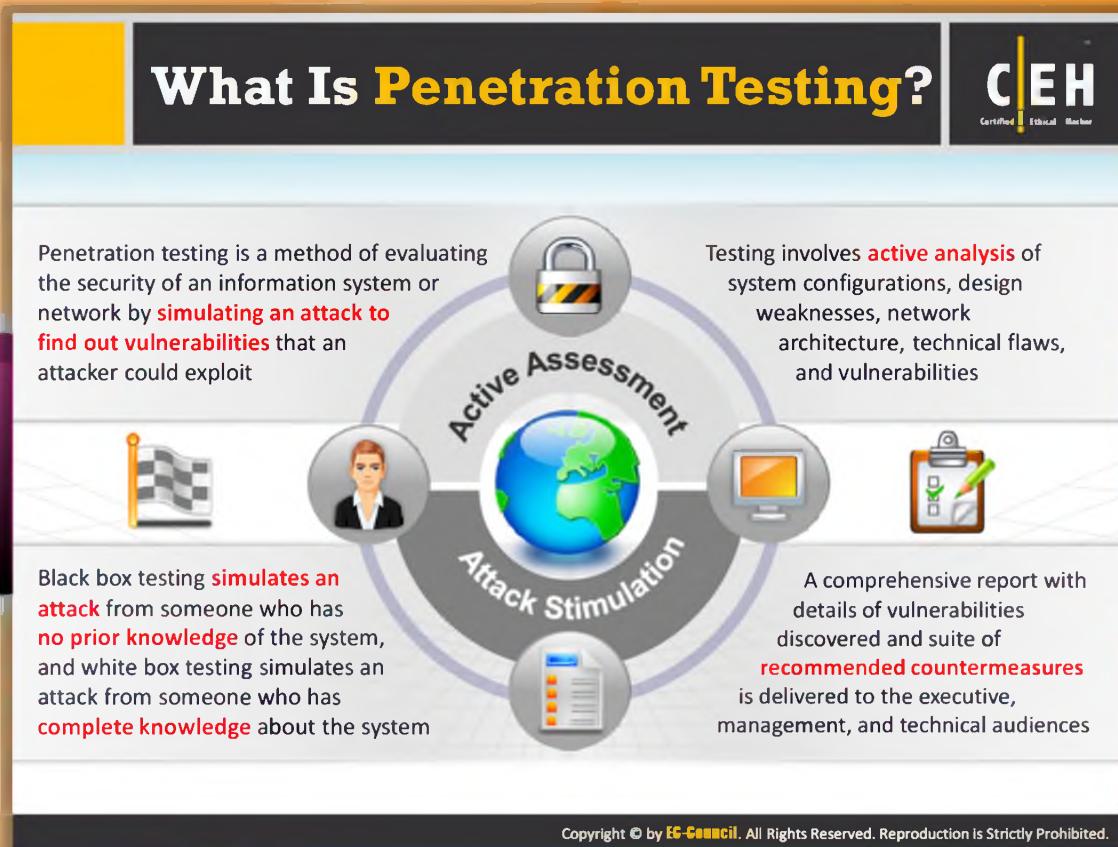
Hacker Journals is an online **Information Security Community**. It propagates news specifically related to information security threats and issues from all over the world. Its research teams search and compile news from tens of thousands of sites to bring you the most relevant Cyber Security titles in one location. In addition to news, it hosts blogs and discussions, education videos, as well as its World Famous Hack.ED column, providing education series in Ethical Hacking and Countermeasure Techniques and technologies.



WindowsSecurity Blogs

Source: <http://blogs.windowsecurity.com>

Windows security has blogs posted by **famous authors** who are leading industry experts. It has various features such as articles and tutorials, blogs, message boards, security tests, and white papers.



What Is Penetration Testing?

Penetration testing is a method of **evaluating security levels** of a particular system or network. This helps you determine the flaws related to **hardware** and **software**. The early identification helps **protect the network**. If the vulnerabilities aren't identified early, then they become an easy source for the attacker for the intrusion.

During penetration testing, a pen tester analyzes all the **security measures** employed by the organization for design weaknesses, technical flaws, and vulnerabilities. There are two types of testing; **black box testing** and **whitebox testing**. Black box testing simulates an attack from someone who is **unfamiliar** with the system, and white box testing simulates an attacker that has **knowledge** about the system. Once all the tests are conducted, the pen tester prepares a report and includes all the test results and the tests conducted along with the vulnerabilities found and the respective countermeasures that can be applied. Finally, the pen tester delivers the report to executive, management, and technical audiences.

Why Penetration Testing

C|EH
Certified Ethical Hacker

The diagram illustrates the benefits of penetration testing using a spiral-bound notebook as a metaphor. The left page contains icons for a person and a lock, while the right page contains icons for a lock and network security devices. A vertical spiral binding connects the two pages.

- Identify the threats facing an organization's information assets
- Reduce an organization's expenditure on IT security and enhance **Return On Security Investment (ROSI)** by identifying and remediating vulnerabilities or weaknesses
- Provide assurance with comprehensive assessment of organization's security including policy, procedure, design, and implementation
- Gain and maintain certification to an **industry regulation (BS7799, HIPAA etc.)**
- Adopt **best practices** in compliance to legal and industry regulations
- For testing and validating the efficiency of **security protections and controls**
- For changing or upgrading **existing infrastructure** of software, hardware, or network design
- Focus on **high-severity vulnerabilities** and emphasize **application-level security issues** to development teams and management
- Provide a comprehensive approach of **preparation steps** that can be taken to prevent upcoming exploitation
- Evaluate the efficiency of **network security devices** such as firewalls, routers, and web servers

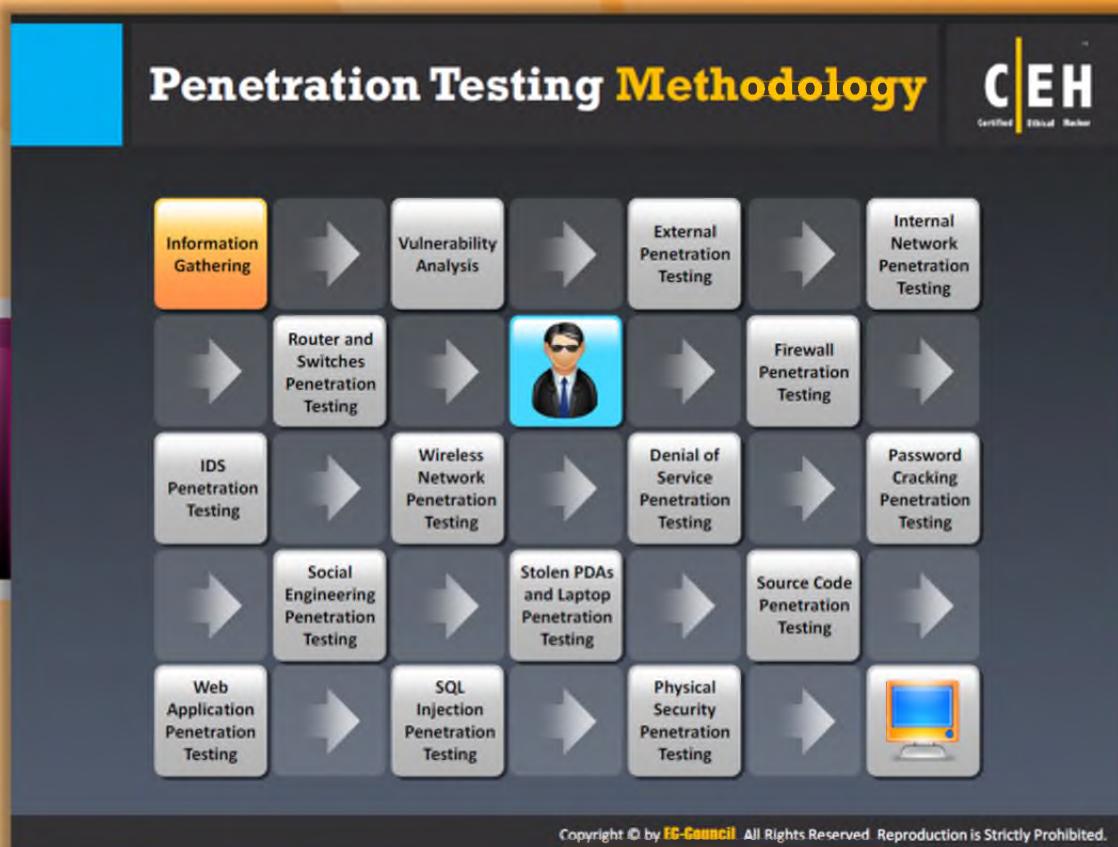
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



Why Penetration Testing?

Penetration testing is required because it helps you to:

- Identify the threats facing an organization's information assets
- Reduce an organization's IT security **costs** and provide a better **Return On Security Investment (ROSI)** by identifying and resolving vulnerabilities and weaknesses
- Provide an organization with assurance: a thorough and comprehensive assessment of organizational security covering policy, procedure, design, and implementation
- Gain and maintain certification to an industry regulation (BS7799, HIPAA etc.)
- Adopt best practices by conforming to **legal** and **industry regulations**
- Test and validate the efficiency of **security protections** and **controls**
- Change or upgrade existing infrastructure of software, hardware, or network design
- Focus on **high-severity vulnerabilities** and emphasize **application-level security** issues to development teams and management
- Provide a comprehensive approach of preparation steps that can be taken to prevent upcoming exploitation
- Evaluate the efficiency of network security devices such as firewalls, routers, and web servers



Penetration Testing Methodology

As a pen tester, you should never overlook any information resource. All possible information sources must be tested for vulnerabilities. Not just the information sources, but every **mechanism** and the **software** involved in your business must be tested because if the attacker is not able to compromise the information system, then he or she may try to gain access to the system and then to the **sensitive information**. A few attacks, such as denial-of-service attacks, don't even need access to the system. Therefore, to ensure that you check all possible ways of compromising a system or network, you should follow the penetration testing methodology. This ensures the full scope of the test.

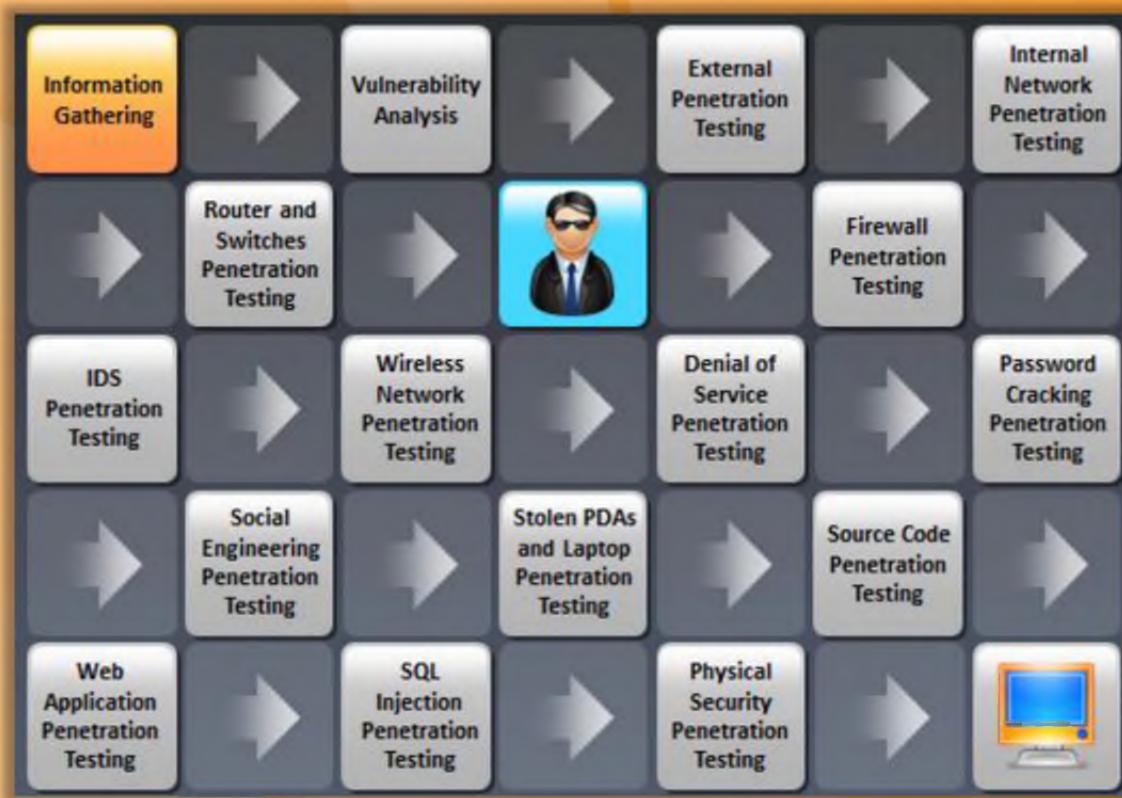
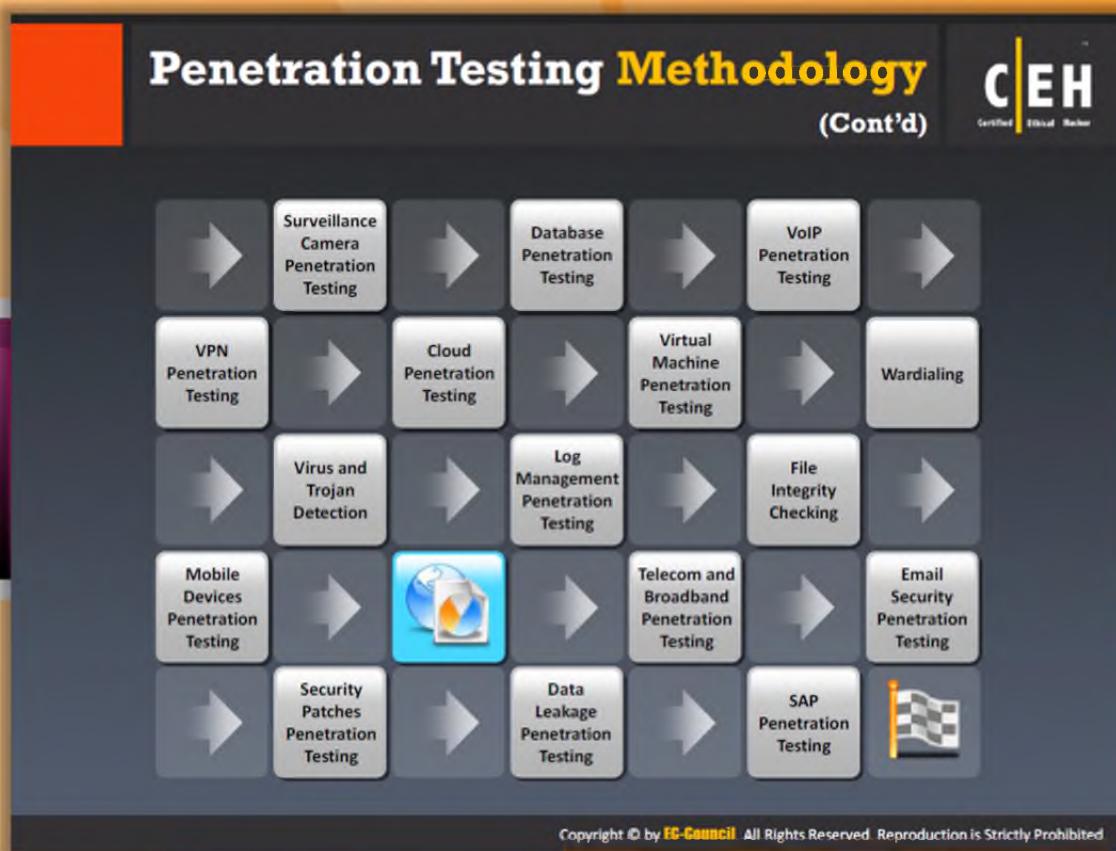


FIGURE 1.5: Penetration Testing Methodology Part -1



Penetration Testing Methodology (Cont'd)



FIGURE 1.6: Penetration Testing Methodology Part -2

Module Summary



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

- ❑ Complexity of security requirements is increasing day by day as a result of evolving technology, changing hacking tactics, emerging security vulnerabilities, etc.
- ❑ Hacker or cracker is one who accesses a computer system by evading its security system
- ❑ Ethical hacking involves the use of hacking tools, tricks, and techniques to identify vulnerabilities so as to ensure system security
- ❑ Ethical hackers help organization to better understand their security systems and identify the risks, highlight the remedial actions, and also reduce ICT costs by resolving those vulnerabilities
- ❑ Ethical hacker should possess platform knowledge, network knowledge, computer expert, security knowledge, and technical knowledge skills
- ❑ Ethical hacking is a crucial component of risk assessment, auditing, counter fraud, best practices, and good governance



Module Summary

This module is summarized as follows:

- ➊ The complexity of **security requirements** is increasing day by day as a result of evolving technology, changing hacking tactics, emerging security vulnerabilities, etc.
- ➋ A hacker or cracker is someone who accesses a computer system by **evading** its **security** system.
- ➌ Ethical hacking involves the use of hacking tools, tricks, and techniques to identify **vulnerabilities** to ensure system security.
- ➍ Ethical hackers help organizations to better understand their security systems and **identify** the **risks**, highlight the **remedial actions**, and also reduce **ICT costs** by resolving those vulnerabilities.
- ➎ An ethical hacker possesses **platform** knowledge, **network** knowledge, **computer** expert, **security** knowledge, and **technical knowledge** skills.
- ➏ Ethical hacking is a crucial component of **risk assessment**, auditing, counter fraud, best practices, and good governance.

Footprinting and Reconnaissance

Module 02



Footprinting and Reconnaissance

Module 02

Engineered by Hackers. Presented by Professionals.



The slide features a dark grey header and footer area. The main title 'Footprinting and Reconnaissance' is in large yellow font. Below it, 'Module 02' is in a smaller white font. The footer contains the slogan 'Engineered by Hackers. Presented by Professionals.' in white. At the bottom, there is a row of five colored icons: black (CEH logo), green (hacker profile), blue (computer monitor), yellow (globe), and orange (file with locks).

Ethical Hacking and Countermeasures v8

Module 02: Footprinting and Reconnaissance

Exam 312-50

The screenshot shows a news article titled "Facebook a 'treasure trove' of Personally Identifiable Information". The article discusses how Facebook contains a "treasure trove" of personally identifiable information that hackers can access. It mentions a report by Imperva that revealed users' "general personal information" can include a date of birth, home address, and mother's maiden name, allowing hackers to create targeted spearphishing campaigns. The article also details a concept called "friend-mapping" where attackers can gain further knowledge of a user's circle of friends. A quote from Noa Bar-Yosef, senior security strategist at Imperva, is included. The URL <http://www.scmagazineuk.com> is visible at the bottom right.

Security News

Facebook a 'treasure trove' of Personally Identifiable Information

Facebook contains a "treasure trove" of personally identifiable information that hackers manage to get their hands on.

A report by Imperva revealed that users' "general personal information" can often include a date of birth, home address and sometimes mother's maiden name, allowing hackers to access this and other websites and applications and create targeted spearphishing campaigns.

It detailed a concept I call "friend-mapping", where an attacker can get further knowledge of a user's circle of friends; having accessed their account and posing as a trusted friend, they can cause mayhem. This can include requesting the transfer of funds and extortion.

Asked why Facebook is so important to hackers, Imperva senior security strategist Noa Bar-Yosef said: "People also add work friends on Facebook so a team leader can be identified and this can lead to corporate data being accessed, project work being discussed openly, while geo-location data can be detailed for military intelligence."

"Hacktivism made up 58 per cent of attacks in the Verizon Data Breach Intelligence Report, and they are going after information on Facebook that can be used to humiliate a person. All types of attackers have their own techniques."

<http://www.scmagazineuk.com>

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



Security News

Facebook a 'treasure trove' of Personally Identifiable Information

Source: <http://www.scmagazineuk.com>

Facebook contains a "treasure trove" of **personally identifiable information** that hackers manage to get their hands on.

A report by Imperva revealed that users' "**general personal information**" can often include a date of birth, home address and sometimes mother's maiden name, allowing hackers to access this and other websites and applications and create targeted **spearphishing** campaigns.

It detailed a concept I call "friend-mapping", where an attacker can get further knowledge of a user's circle of friends; having accessed their account and posing as a trusted friend, they can cause mayhem. This can include requesting the transfer of funds and extortion.

Asked why Facebook is so important to hackers, **Imperva senior security** strategist Noa Bar-Yosef said: "People also add work friends on Facebook so a team leader can be identified and this can lead to corporate data being accessed, project work being discussed openly, while geo-location data can be detailed for military intelligence."

"Hacktivism made up 58 per cent of attacks in the **Verizon Data Breach Intelligence Report**, and they are going after information on Facebook that can be used to humiliate a person. All types of attackers have their own techniques."

On how attackers get a password in the first place, Imperva claimed that different **keyloggers** are used, while phishing kits that create a **fake Facebook login page** have been seen, and a more primitive method is a brute force attack, where the attacker repeatedly attempts to guess the user's password.

In more extreme cases, a **Facebook administrator's** rights can be accessed. Although it said that this requires more effort on the hacker side and is not as prevalent, it is the "**holy grail**" of attacks as it provides the hacker with data on all users.

On protection, Bar-Yosef said the roll-out of SSL across the whole website, rather than just at the login page, was effective, but users still needed to opt into this.



By Dan Raywood

<http://www.scmagazine.com.au/Feature/265065,digital-investigations-have-matured.aspx>

Module Objectives

C|EH
Certified Ethical Hacker

- Footprinting Terminology
- What Is Footprinting?
- Objectives of Footprinting
- Footprinting Threats
- Footprinting through Search Engines
- Website Footprinting
- Email Footprinting
- Competitive Intelligence
- Footprinting Using Google

- WHOIS Footprinting
- DNS Footprinting
- Network Footprinting
- Footprinting through Social Engineering
- Footprinting through Social Networking Sites
- Footprinting Tools
- Footprinting Countermeasures
- Footprinting Pen Testing



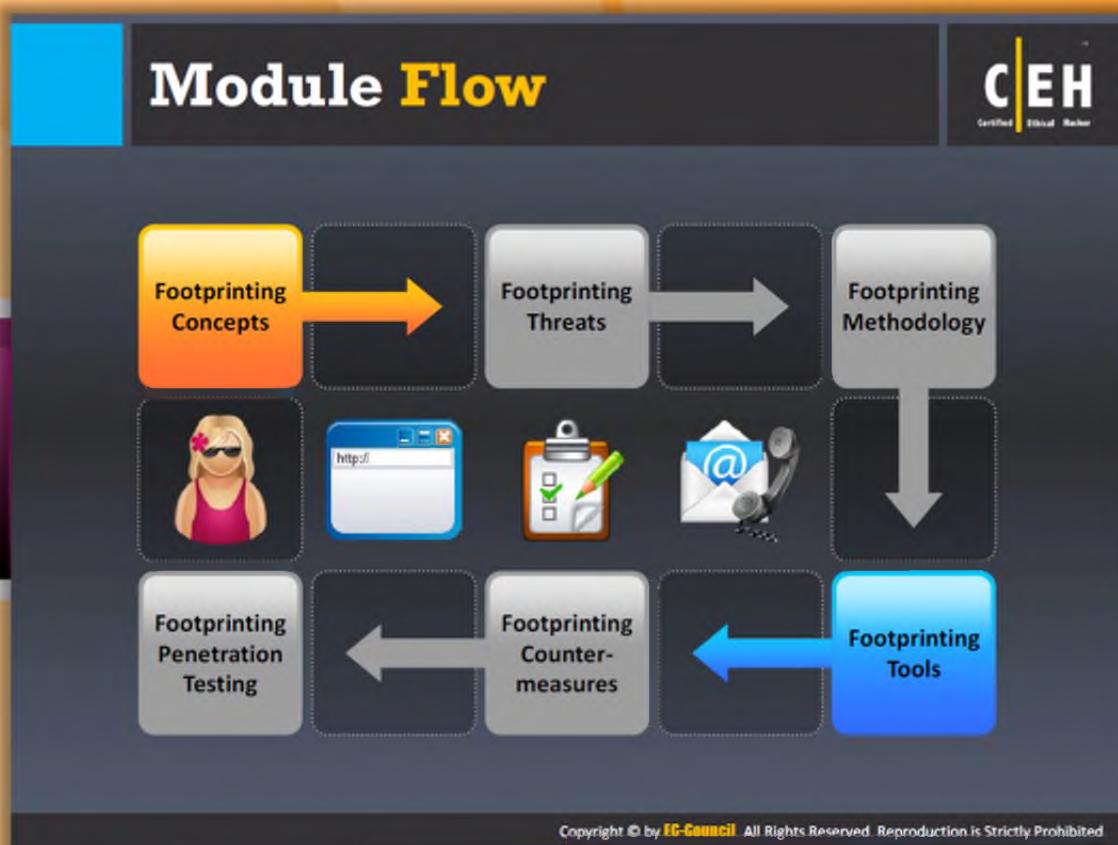
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



Module Objectives

This module will make you familiarize with the following:

- | | |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none">■ Footprinting Terminologies■ What Is Footprinting?■ Objectives of Footprinting■ Footprinting Threats■ Footprinting through Search Engines■ Website Footprinting■ Email Footprinting■ Competitive Intelligence■ Footprinting Using Google | <ul style="list-style-type: none">■ WHOIS Footprinting■ DNS Footprinting■ Network Footprinting■ Footprinting through Social Engineering■ Footprinting through Social Networking Sites■ Footprinting Tools■ Footprinting Countermeasures■ Footprinting Pen Testing |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|



Module Flow

Ethical hacking is legal hacking conducted by a penetration tester in order to evaluate the security of an **IT infrastructure** with the permission of an organization. The concept of ethical hacking cannot be explained or cannot be performed in a single step; therefore, it has been divided into several steps. Footprinting is the first step in ethical hacking, where an attacker tries to gather information about a target. To help you better **understand footprinting**, it has been distributed into various sections:

Footprinting Concepts	Footprinting Tools
Footprinting Threats	Footprinting Countermeasures
Footprinting Methodology	Footprinting Penetration Testing

The **Footprinting Concepts** section familiarizes you with footprinting, footprinting terminology, why footprinting is necessary, and the objectives of footprinting.

Footprinting Terminology

Open Source or Passive Information Gathering
Collect information about a target from the **publicly accessible sources**

Active Information Gathering
Gather information through **social engineering** on-site visits, interviews, and questionnaires

Anonymous Footprinting
Gather information from sources where the **author of the information** cannot be identified or traced

Pseudonymous Footprinting
Collect information that might be **published under a different name** in an attempt to preserve privacy

Organizational or Private Footprinting
Collect information from an **organization's web-based calendar** and **email services**

Internet Footprinting
Collect information about a target from the **Internet**

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



Footprinting Terminology

Before going deep into the concept, it is important to know the basic terminology used in footprinting. These terms help you understand the concept of footprinting and its structures.



Open Source or Passive Information Gathering

Open source or passive information gathering is the easiest way to collect information about the target organization. It refers to the process of gathering information from the open sources, i.e., publicly available sources. This requires no direct contact with the **target organization**. Open sources may include newspapers, television, social networking sites, blogs, etc.

Using these, you can gather information such as network boundaries, IP address reachable via the Internet, operating systems, web server software used by the target network, TCP and UDP services in each system, access control mechanisms, system architecture, intrusion detection systems, and so on.



Active Information Gathering

In active information gathering, process attackers mainly focus on the employees of

the target organization. Attackers try to extract information from the employees by conducting **social engineering**: on-site visits, interviews, questionnaires, etc.



Anonymous Footprinting

This refers to the process of collecting information from sources anonymously so that your efforts cannot be traced back to you.



Pseudonymous Footprinting

Pseudonymous footprinting refers to the process of collecting information from the sources that have been published on the Internet but is not directly linked to the **author's name**. The information may be published under a different name or the author may have a well-established pen name, or the author may be a corporate or government official and be prohibited from posting under his or her original name. Irrespective of the reason for hiding the author's name, collecting information from such sources is called **pseudonymous**.



Organizational or Private Footprinting

Private footprinting involves collecting information from an organization's **web-based calendar** and email services.



Internet Footprinting

Internet footprinting refers to the process of collecting information of the target organization's connections to the Internet.

What Is Footprinting?

Footprinting is the process of **collecting** as much information as possible about a target network, for identifying various ways to intrude into an **organization's network system**



Process Involved in Footprinting a Target

- 1 Collect basic information about the target and its network
- 2 Determine the operating system used, platforms running, web server versions, etc.
- 3 Perform techniques such as Whois, DNS, network and organizational queries
- 4 Find vulnerabilities and exploits for launching attacks

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



What Is Footprinting?

Footprinting, the first step in ethical hacking, refers to the process of collecting information about a target network and its environment. Using footprinting you can find various ways to intrude into the target organization's network system. It is considered "**methodological**" because critical information is sought based on a previous discovery.

Once you begin the footprinting process in a methodological manner, you will obtain the blueprint of the security profile of the target organization. Here the term "**blueprint**" is used because the result that you get at the end of footprinting refers to the unique system profile of the target organization.

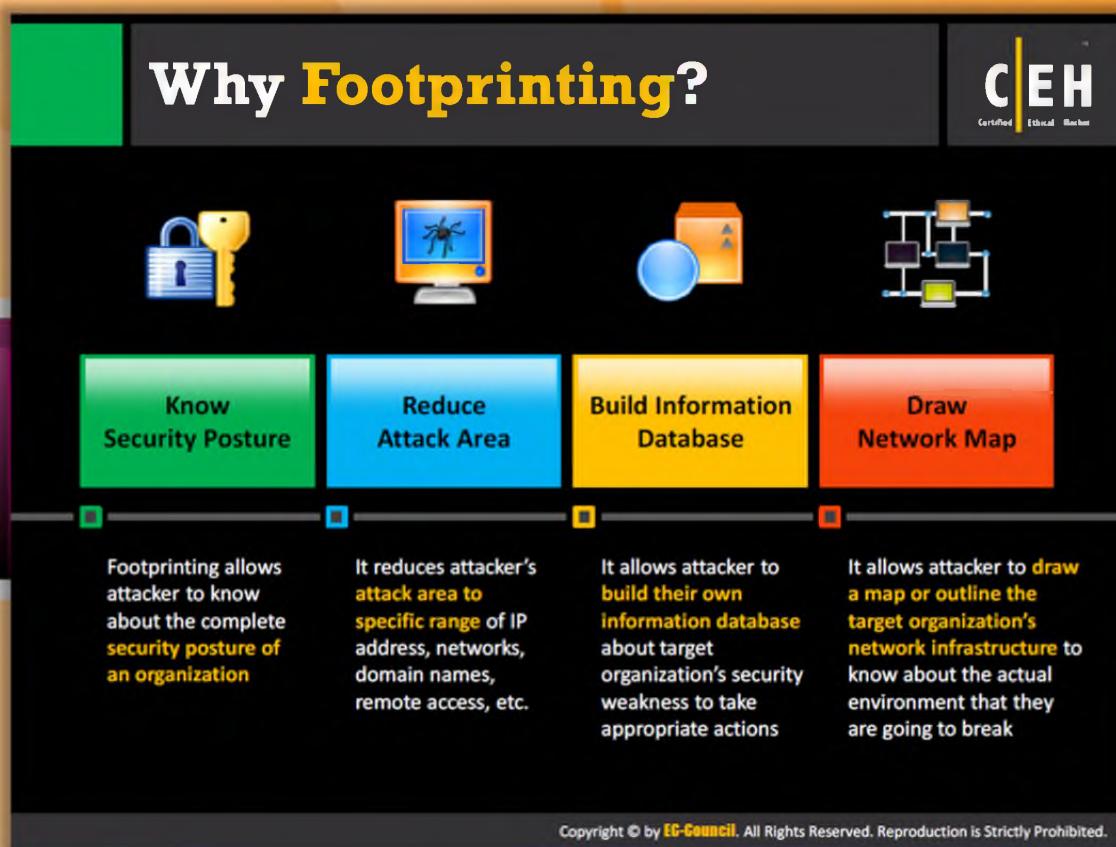
There is no single methodology for footprinting as you can trace information in several routes. However, this activity is important as all crucial information needs to be gathered before you begin hacking. Hence, you should carry out the footprinting precisely and in an **organized manner**.

You can collect information about the target organization through the means of footprinting in four steps:

1. Collect basic information about the target and its network
2. Determine the operating system used, platforms running, web server versions, etc.

3. Perform techniques such as Whois, DNS, network and organizational queries
4. Find vulnerabilities and exploits for launching attacks

Furthermore, we will discuss how to collect basic information, determine operating system of target computer, platforms running, and web server versions, various methods of footprinting, and how to find and **exploit vulnerabilities** in detail.



Why Footprinting?

For attackers to build a hacking strategy, they need to gather information about the target organization's network, so that they can find the easiest way to break into the **organization's security perimeter**. As mentioned previously, footprinting is the easiest way to gather information about the target organization; this plays a vital role in the hacking process.

Footprinting helps to:

- **Know Security Posture**

Performing footprinting on the target organization in a systematic and methodical manner gives the complete profile of the organization's security posture. You can analyze this report to figure out loopholes in the security posture of your target organization and then you can build your **hacking plan** accordingly.

- **Reduce Attack Area**

By using a combination of tools and techniques, attackers can take an unknown entity (for example XYZ Organization) and reduce it to a specific range of domain names, network blocks, and individual IP addresses of systems directly connected to the Internet, as well as many other details pertaining to its **security posture**.

- **Build Information Database**

A detailed footprint provides maximum information about the target organization. Attackers can build their own information database about security weakness of the target organization. This database can then be analyzed to find the easiest way to break into the organization's security perimeter.

- **Draw Network Map**

Combining footprinting techniques with tools such as Tracert allows the attacker to create network diagrams of the target organization's network presence. This network map represents their understanding of the **target's Internet footprint**. These network diagrams can guide the attack.



Objectives of Footprinting

The major objectives of footprinting include collecting the **target's network information**, system information, and the organizational information. By carrying out footprinting at various network levels, you can gain information such as: network blocks, network services and applications, system architecture, intrusion detection systems, specific IP addresses, and access control mechanisms. With footprinting, information such as employee names, phone numbers, contact addresses, designation, and work experience, and so on can also be obtained.



Collect Network Information

The network information can be gathered by performing a **Whois database analysis**, **trace routing**, etc. includes:

- Domain name
- Internal domain names
- Network blocks
- IP addresses of the reachable systems
- Rogue websites/private websites

- ⌚ TCP and UDP services running
- ⌚ Access control mechanisms and ACLs
- ⌚ Networking protocols
- ⌚ VPN points
- ⌚ ACLs
- ⌚ IDSes running
- ⌚ Analog/digital telephone numbers
- ⌚ Authentication mechanisms
- ⌚ System enumeration



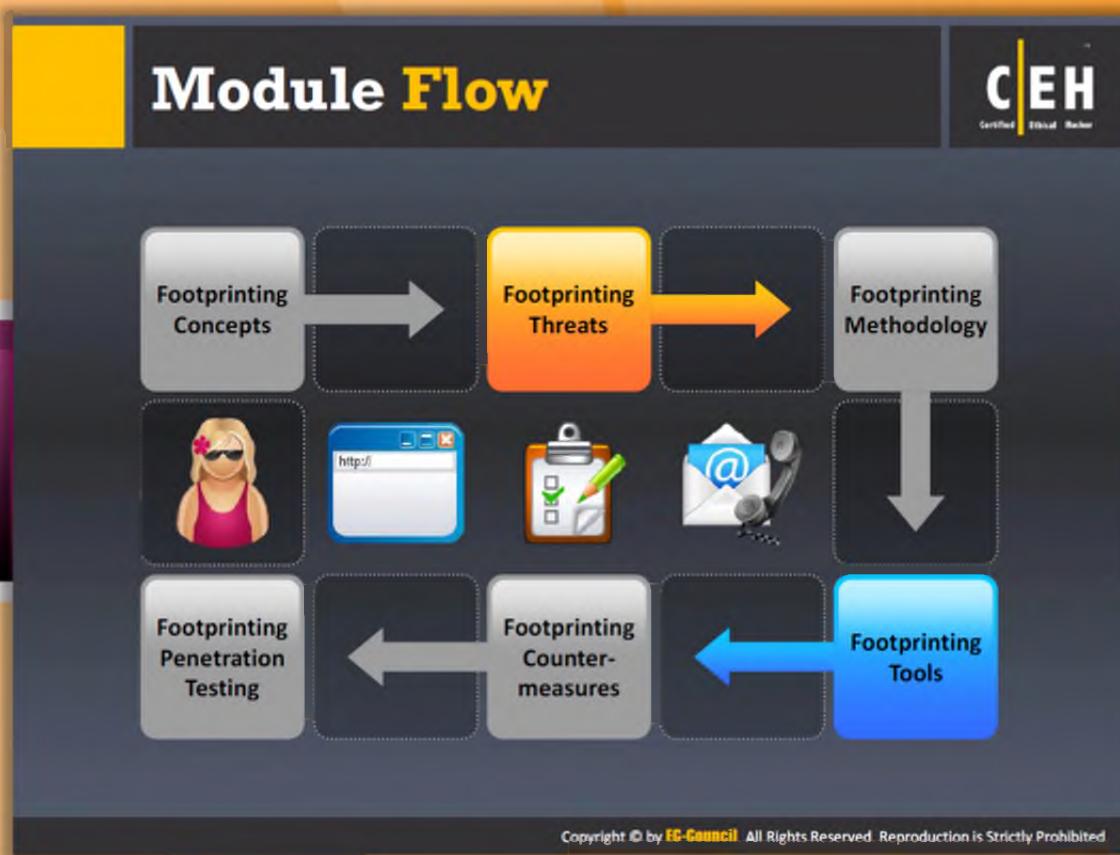
Collect System Information

- ⌚ User and group names
- ⌚ System banners
- ⌚ Routing tables
- ⌚ SNMP information
- ⌚ System architecture
- ⌚ Remote system type
- ⌚ System names
- ⌚ Passwords



Collect Organization's Information

- ⌚ Employee details
- ⌚ Organization's website
- ⌚ Company directory
- ⌚ Location details
- ⌚ Address and phone numbers
- ⌚ Comments in HTML source code
- ⌚ Security policies implemented
- ⌚ Web server links relevant to the organization
- ⌚ Background of the organization
- ⌚ News articles/press releases



Module Flow

So far, we discussed footprinting concepts, and now we will discuss the threats associated with footprinting:

 Footprinting Concepts	 Footprinting Tools
 Footprinting Threats	 Footprinting Countermeasures
 Footprinting Methodology	 Footprinting Penetration Testing

The Footprinting Threats section familiarizes you with the threats associated with footprinting such as social engineering, system and network attacks, corporate espionage, etc.

Footprinting Threats

C|EH
Certified Ethical Hacker

Attackers gather valuable **system and network information** such as account details, operating system and installed applications, network components, server names, database schema details, etc. from footprinting techniques



Types of Threats

- Social Engineering
- System and Network Attacks
- Information Leakage
- Privacy Loss
- Corporate Espionage
- Business Loss



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



Footprinting Threats

As discussed previously, attackers perform footprinting as the first step in an attempt to **hack a target organization**. In the footprinting phase, attackers try to collect valuable system-level information such as account details, operating system and other software versions, server names, and database schema details that will be useful in the hacking process.

The following are various threats due to footprinting:



Social Engineering

Without using any intrusion methods, hackers directly and indirectly collect information through persuasion and various other means. Here, crucial information is gathered by the **hackers** through **employees** without their consent.



System and Network Attacks

Footprinting helps an attacker to perform system and network attacks. Through **footprinting**, **attackers** can gather information related to the target organization's system configuration, operating system running on the machine, and so on. Using this information, attackers can find the vulnerabilities present in the target system and then can exploit those

vulnerabilities. Thus, attackers can take control over a target system. Similarly, attackers can also take control over the entire network.



Information Leakage

Information leakage can be a great threat to any organization and is often overlooked. If sensitive organizational information falls into the hands of attackers, then they can build an attack plan based on the information, or use it for **monetary benefits**.



Privacy Loss

With the help of footprinting, hackers are able to access the systems and networks of the company and even escalate the privileges up to admin levels. Whatever **privacy** was maintained by the company is completely lost.



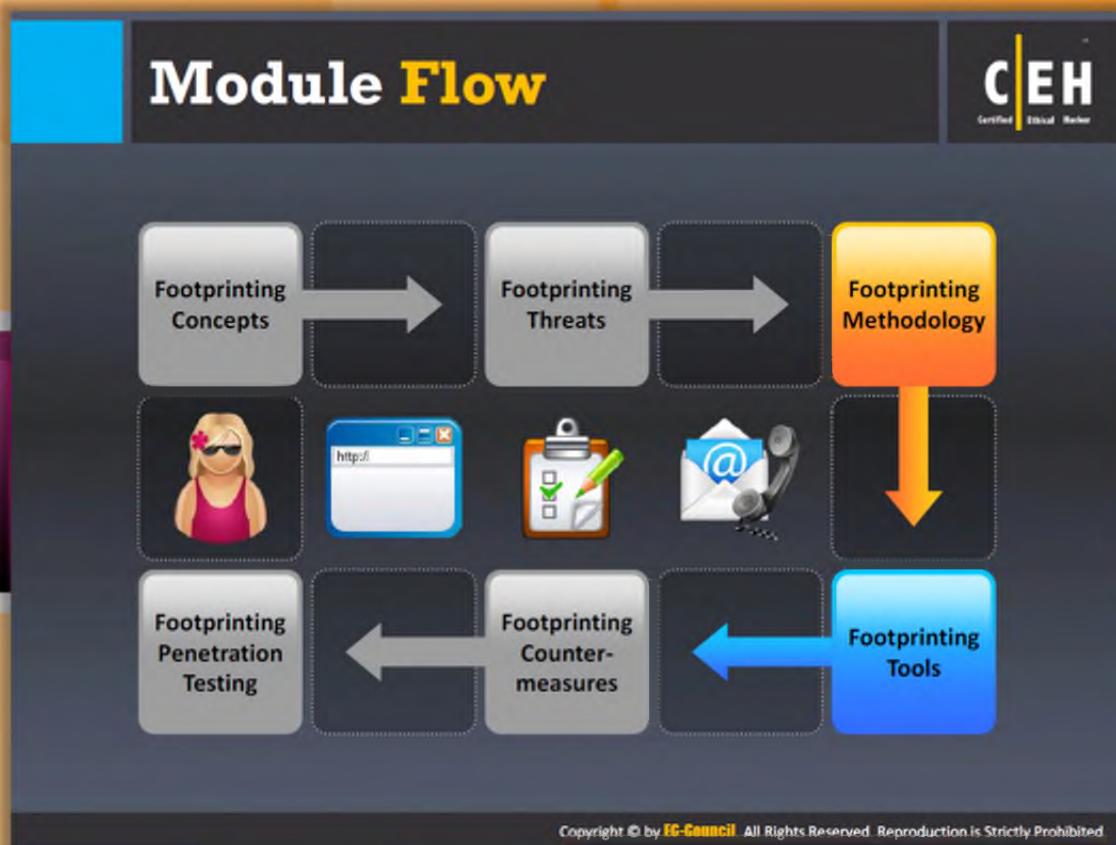
Corporate Espionage

Corporate espionage is one of the major threats to companies as competitors can **spy** and attempt to steal **sensitive data** through footprinting. Due to this type of espionage, competitors are able to launch similar products in the market, affecting the market position of a company.



Business Loss

Footprinting has a major effect on businesses such as online businesses and other **ecommerce websites**, banking and financial related businesses, etc. Billions of dollars are lost every year due to malicious attacks by hackers.



Module Flow

Now that you are familiar with footprinting concepts and threats, we will discuss the footprinting methodology.

The footprinting methodology section discusses various techniques used to collect information about the **target organization** from different sources.

Footprinting Concepts	Footprinting Tools
Footprinting Threats	Footprinting Countermeasures
Footprinting Methodology	Footprinting Penetration Testing



Footprinting Methodology

The footprinting methodology is a procedural way of **collecting information** about a target organization from all available sources. It deals with gathering information about a target organization, determining URL, location, establishment details, number of employees, the specific range of domain names, and contact information. This information can be gathered from various sources such as search engines, Whois databases, etc.

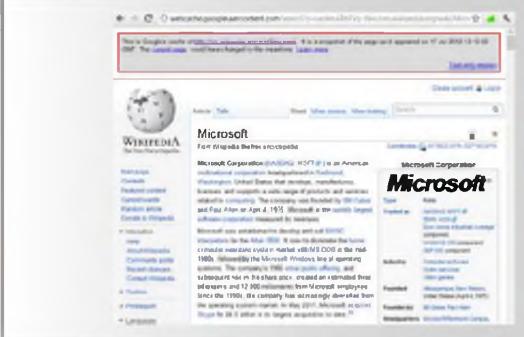
Search engines are the main information sources where you can find valuable information about your **target organization**. Therefore, first we will discuss footprinting through search engines. Here we are going to discuss how and what information we can collect through search engines.

Examples of search engines include: www.google.com, www.yahoo.com, www.bing.com

Footprinting through Search Engines

C|EH
Certified Ethical Hacker

- Attackers use search engines to **extract information about a target** such as technology platforms, employee details, login pages, intranet portals, etc. which helps in performing social engineering and other types of advanced system attacks
- Search engine **cache may provide sensitive information** that has been removed from the World Wide Web (WWW)



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



Footprinting through Search Engines

A web search engine is designed to search for information on the World Wide Web. The search results are generally presented in a line of results often referred to as search engine results pages (SERPs). In the present world, many search engines allow you to extract a target organization's information such as technology platforms, employee details, login pages, intranet portals, and so on. Using this information, an attacker may build a **hacking strategy** to break into the target organization's network and may carry out other types of advanced system attacks. A Google search could reveal submissions to forums by security personnel that reveal brands of firewalls or **antivirus software** in use at the target. Sometimes even network diagrams are found that can guide an attack.

If you want to footprint the target organization, for example XYZ pvt Ltd, then type XYZ pvt Ltd in the Search box of the search engine and press Enter. This will display all the search results containing the keywords "XYZ pvt Ltd." You can even narrow down the results by adding a specific keyword while searching. Furthermore, we will discuss other **footprinting techniques** such as website footprinting and email Footprinting.

For example, consider an organization, perhaps Microsoft. Type Microsoft in the Search box of a search engine and press Enter; this will display all the results containing information about Microsoft. Browsing the results may provide critical information such as **physical location**,

contact address, the services offered, number of employees, etc. that may prove to be a valuable source for hacking.

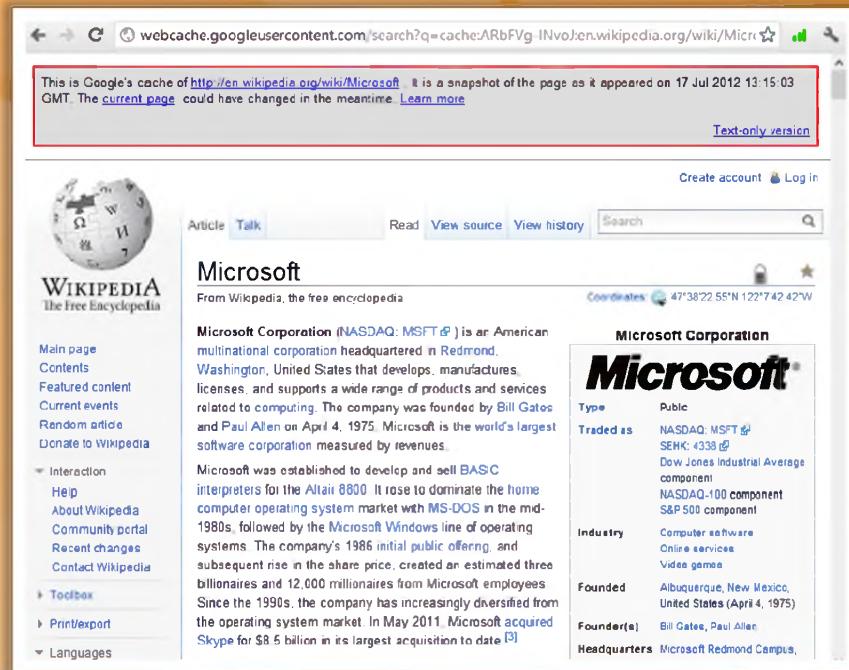


FIGURE 2.1: Screenshot showing information about Microsoft

As an ethical hacker, if you find any **sensitive information** of your company in the search engine result pages, you should remove that information. Although you remove the sensitive information, it may still be available in a search engine cache. Therefore, you should also check the search engine cache to ensure that the sensitive data is removed **permanently**.

Finding Company's External and Internal URLs

C|EH
Certified Ethical Hacker

- Search for the target company's external URL in a search engine such as [Google](#) or [Bing](#)
- Internal URLs provide an insight into different departments and business units in an organization
- You may find an internal company's URL by trial and error method

Tools to Search Internal URLs

- <http://news.netcraft.com>
- <http://www.webmaster-a.com/link-extractor-internal.php>



Internal URL's of microsoft.com

- support.microsoft.com
- office.microsoft.com
- search.microsoft.com
- msdn.microsoft.com
- update.microsoft.com
- technet.microsoft.com
- windows.microsoft.com



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



Finding Company's External and Internal URLs

A company's external and internal URLs provide a lot of useful information to the attacker. These URLs describe the company and provide details such as the company mission and vision, history, products or services offered, etc. The URL that is used **outside the corporate network** for accessing the company's vault server via a firewall is called an external URL. It links directly to the company's external web page. The target company's external URL can be determined with the help of search engines such as [Google](#) or [Bing](#).

If you want to find the external URL of a company, follow these steps:

1. Open any of the search engines, such as Google or Bing.
2. Type the name of the target company in the Search box and press Enter.

The internal URL is used for accessing the company's vault server directly inside the corporate network. The internal URL helps to access the internal functions of a company. Most companies use common formats for internal URLs. Therefore, if you know the **external URL** of a company, you can predict an internal URL through trial and error. These internal URLs provide insight into different departments and business units in an organization. You can also find the internal URLs of an organization using tools such as netcraft.

Tools to Search Internal URLs

Netcraft



Source: <http://news.netcraft.com>

Netcraft deals with web server, web **hosting market-share** analysis, and operating system detection. It provides free anti-phishing toolbar (Net craft toolbar) for Firefox as well as Internet Explorer browsers. The netcraft toolbar avoids phishing attacks and protects the Internet users from fraudsters. It checks the risk rate as well as the hosting location of the websites we visit.



Link Extractor

Source: <http://www.webmaster-a.com/link-extractor-internal.php>

Link Extractor is a link extraction utility that allows you to choose between external and internal URLs, and will return a plain list of URLs linked to or an html list. You can use this utility to **competitor sites**.

Examples of internal URLs of microsoft.com:

- ⌚ support.microsoft.com
- ⌚ office.microsoft.com
- ⌚ search.microsoft.com
- ⌚ msdn.microsoft.com
- ⌚ update.microsoft.com
- ⌚ technet.microsoft.com
- ⌚ windows.microsoft.com

Public and Restricted Websites

CEH
Certified Ethical Hacker

Identify a company's private and public websites

The screenshot displays four Microsoft websites arranged in a 2x2 grid:

- Public Website:** <http://www.microsoft.com> (Left)
- Restricted Website:** <http://technet.microsoft.com> (Top Left)
- Restricted Website:** <http://windows.microsoft.com> (Top Right)
- Restricted Website:** <http://office.microsoft.com> (Bottom Left)
- Restricted Website:** <http://answers.microsoft.com> (Bottom Right)

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



Public and Restricted Websites

A public website is a website designed to show the presence of an organization on the Internet. It is designed to attract **customers** and **partners**. It contains information such as company history, services and products, and contact information of the organization.

The following screenshot is an example of a public website:

Source: <http://www.microsoft.com>



FIGURE 2.2: An example of public website

A restricted website is a website that is available to only a few people. The people may be employees of an organization, members of a department, etc. **Restrictions** can be applied based on the IP number, domain or subnet, username, and password.

Restricted or private websites of microsoft.com include: <http://technet.microsoft.com>, <http://windows.microsoft.com>, <http://office.microsoft.com>, and <http://answers.microsoft.com>.

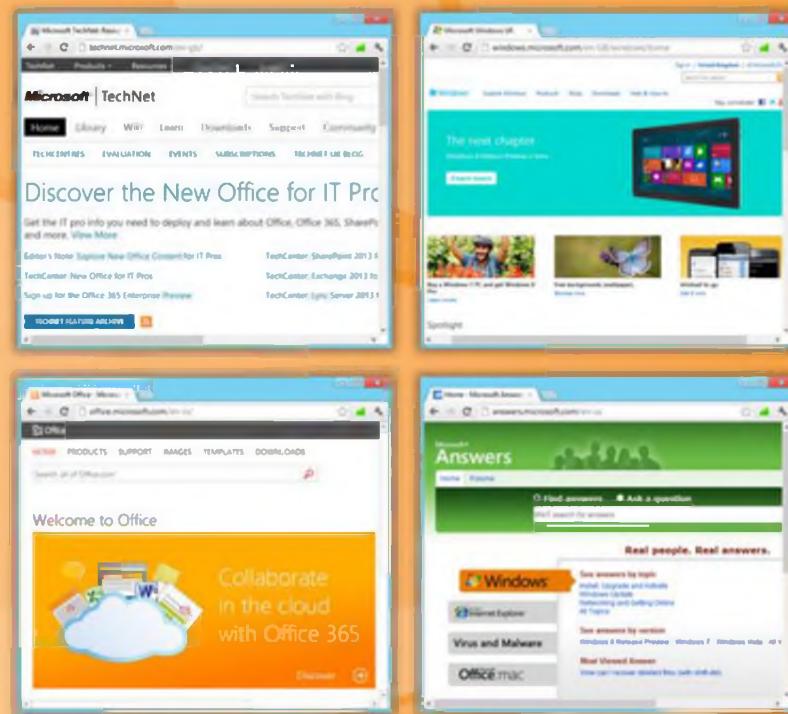


FIGURE 2.3: Examples of Public and Restricted websites

Collect Location Information

CEH
Certified Ethical Hacker

Use Google Earth tool to get the location of the place

Google

The image shows two side-by-side screenshots of the Google Earth application. The left screenshot displays a 3D rendering of the White House and its surrounding grounds. The right screenshot shows a detailed view of the Statue of Liberty and its pedestal. Both images are overlaid with a semi-transparent black box containing text and logos.

<http://earth.google.com>

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



Collect Location Information

Information such as physical location of the organization plays a vital role in the hacking process. This information can be obtained using the footprinting technique. In addition to physical location, we can also collect information such as surrounding public Wi-Fi hotspots that may prove to be a way to break into the **target organization's network**.

Attackers with the knowledge of a target organization's location may attempt dumpster diving, surveillance, social engineering, and other non-technical attacks to gather much more information about the target organization. Once the location of the target is known, detailed satellite images of the location can be obtained using various sources available on the Internet such as <http://www.google.com/earth> and <https://maps.google.com>. Attackers can use this information to gain **unauthorized access** to buildings, wired and wireless networks, systems, and so on.

Example: earth.google.com

Google Earth is a valuable tool for **hacking** that allows you to find a location, point, and zoom into that location to explore. You can even **access 3D images** that depict most of the Earth in high-resolution detail.

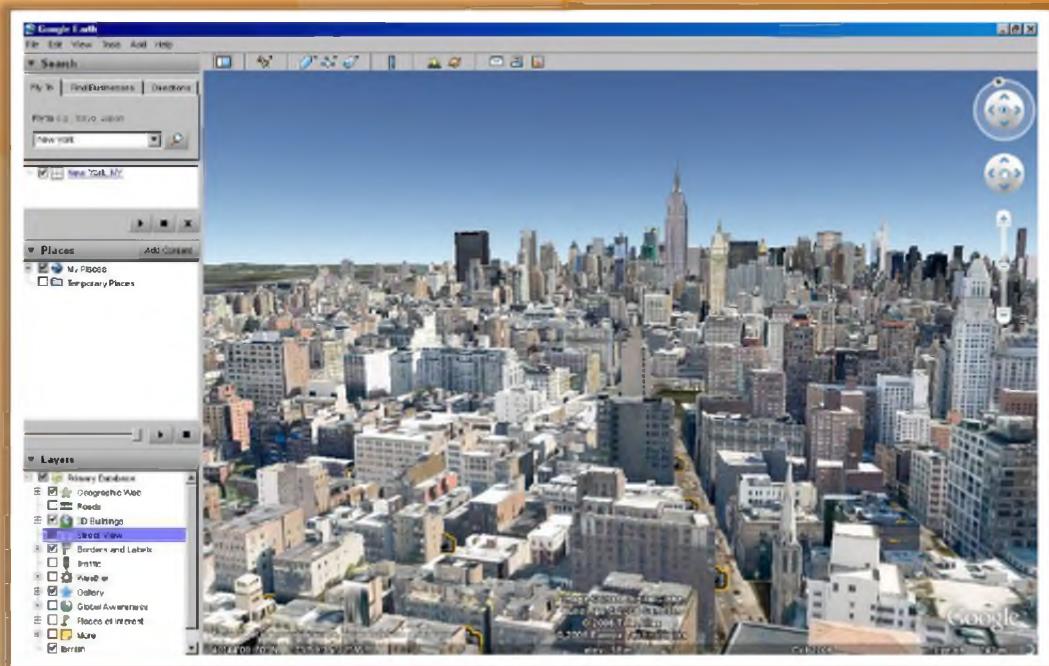


FIGURE 2.4: Google Earth showing location

Example: maps.google.com

Google Maps provides a Street View feature that provides you with a series of images of building, as well as its surroundings, including **WI-FI networks**. Attackers may use Google Maps to find or locate entrances to buildings, security cameras, gates, places to hide, weak spots in perimeter fences, and utility resources like electricity connections, to measure distance between different objects, etc.

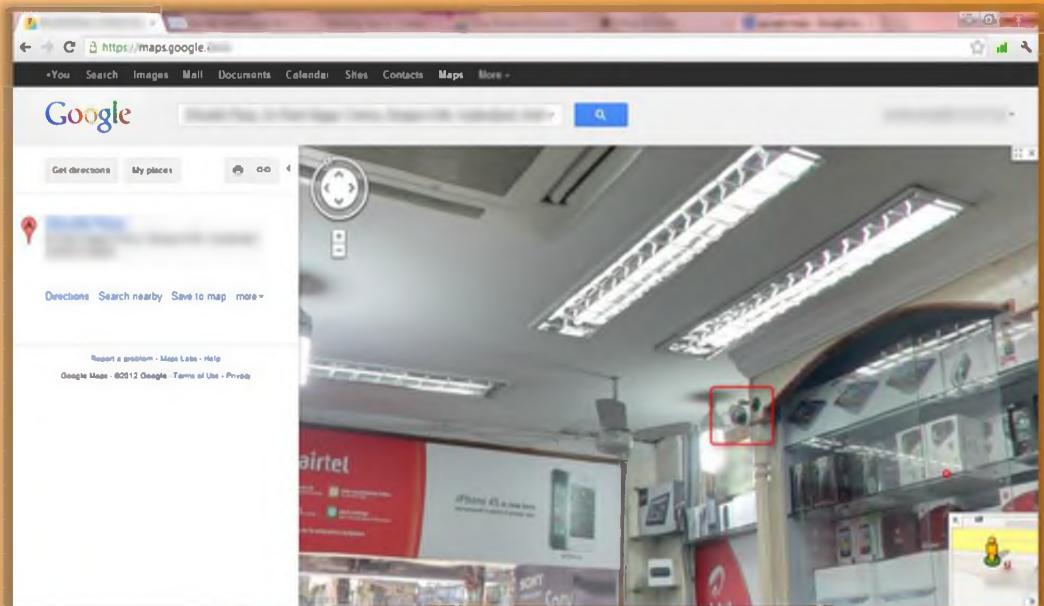


FIGURE 2.5: Google Maps showing a Street View

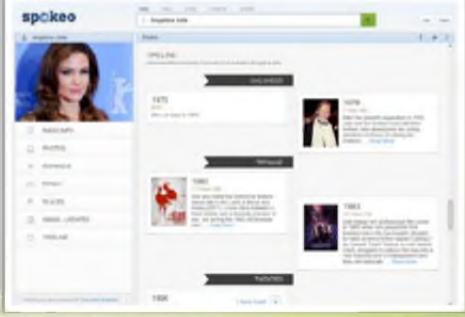
People Search

The people search returns the following information about a person:

- Residential addresses and email addresses
- Contact numbers and date of birth
- Photos and social networking profiles
- Blog URLs
- Satellite pictures of private residences



<http://pipl.com>



<http://www.spokeo.com>

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



People Search

You can use the public record websites to find information about people's email addresses, phone numbers, house addresses, and other information. Using this information you can try to obtain bank details, credit card details, mobile numbers, past history, etc. There are many people search online services available that help find people. <http://pipl.com> and <http://www.spokeo.com> are examples of people search services that allow you to search for the people with their name, email, username, phone, or address.

These people search services may provide information such as:

- Residential addresses and email addresses
- Contact numbers and date of birth
- Photos and social networking profiles
- Blog URLs
- Satellite pictures of **private residences**

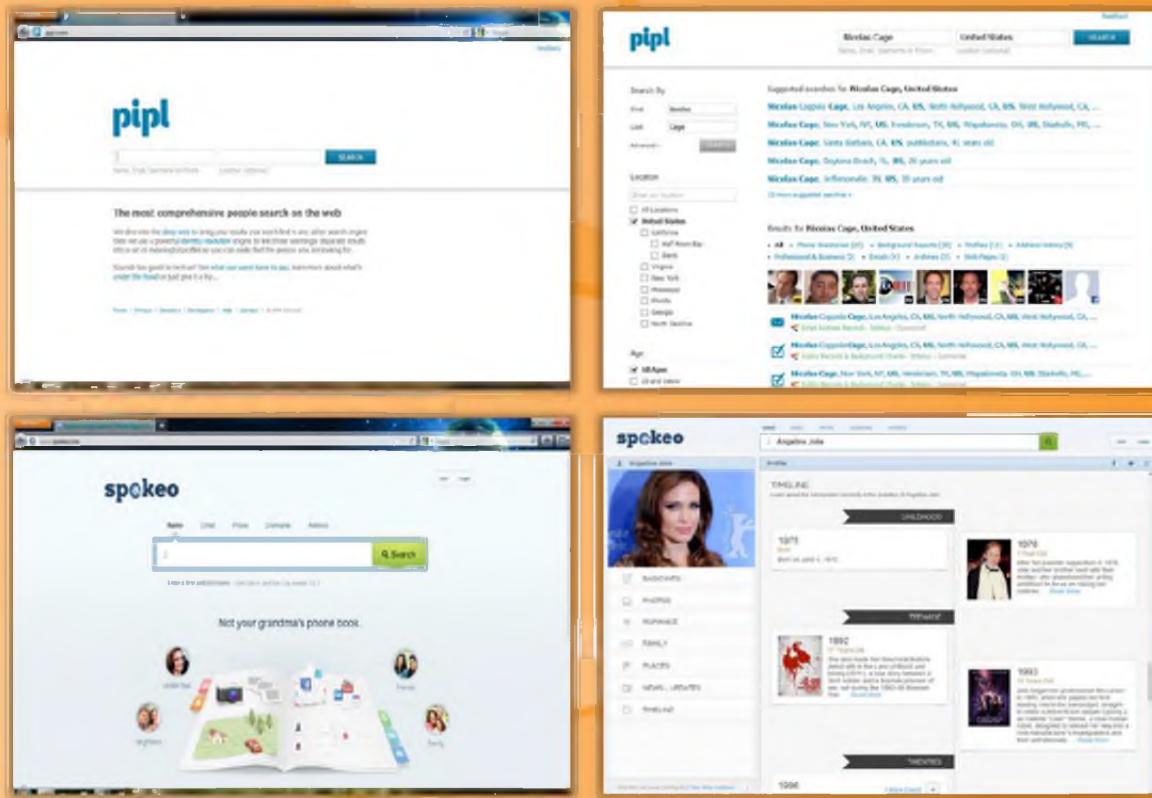


FIGURE 2.6: Examples of People search online service websites

People Search Online Services



Zaba Search <http://www.zabasearch.com>

123 People Search <http://www.123people.com>

ZoomInfo <http://www.zoominfo.com>

PeekYou <http://www.peekyou.com>

Wink People Search <http://wink.com>

Intelius <http://www.intelius.com>

AnyWho <http://www.anywho.com>

PeopleSmart <http://www.peoplesmart.com>

People Lookup <https://www.peoplelookup.com>

WhitePages <http://www.whitepages.com>

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



People Search Online Services

At present, many Internet users are using people search engines to find information about other people. Most often people search engines provide **people's names, addresses, and contact details**. Some people search engines may also reveal the type of work an individual does, businesses owned by a person, contact numbers, company email addresses, mobile numbers, fax numbers, dates of birth, personal -mail addresses, etc. This information proves to be highly beneficial for attackers to launch attacks.

Some of the people search engines are listed as follows:



Zaba Search

Source: <http://www.zabasearch.com>

Zaba Search is a people search engine that provides information such as address, phone number, current location, etc. of people in the US. It allows you to search for people by their name.



ZoomInfo

Source: <http://www.zoominfo.com>

Zoom Info is a business people directory using which you can find business contacts, people's professional profiles, biographies, work histories, affiliations, links to **employee profiles** with verified contact information, and more.



Wink People Search

Source: <http://wink.com>

Wink People Search is a people search engine that provides information about people by name and location. It gives phone number, address, websites, photos, work, school, etc.



AnyWho

Source: <http://www.anywho.com>

AnyWho is a website that helps you find information about people, their businesses, and their locations online. With the help of a **phone number**, you can get all the details of an individual.



People Lookup

Source: <https://www.peoplelookup.com>

People Lookup is a people search engine that allows you to find, locate, and then connect with people. It also allows you to look up a phone number, search for cell numbers, find an address or phone number, and search for people in the US. This **database** uses information from **public records**.



123 People Search

Source: <http://www.123people.com>

123 People Search is a people search tool that allows you to find information such as public records, phone numbers, addresses, images, videos, and email addresses.



PeekYou

Source: <http://www.peekyou.com>

PeekYou is a people search engine that allows you to search for profiles and contact information of people in India and cities' top **employers** and **schools**. It allows you to search for the people with their names or usernames.



Intelius

Source: <http://www.intelius.com>

Intelius is a public records business that provides information services. It allows you to search for the people in US with their name, address, phone number, or **email address**.



PeopleSmart

Source: <http://www.peoplesmart.com>

People Smart is a people search service that allows you to find people's work information with their name, city, and state. In addition, it allows you to perform **reverse phone lookups**, email searches, searches by address, and county searches.



WhitePages

Source: <http://www.whitepages.com>

WhitePages is a people search engine that provides information about people by name and location. Using the phone number, you can find the **person's address**.

People Search on Social Networking Services

The collage displays four examples of people search results:

- Facebook:** A profile page for "Clement Electric - Alber". It shows basic info like address, phone number, and email, along with a detailed "About" section.
- LinkedIn:** A profile page for "Iland Pitt" under the title "Sales & Business Development Executive". It includes a photo, work experience at IBM, education at University of Michigan College Park, and various connections.
- Twitter:** A profile page for "Kate Winslet @OfficialWinslet". It shows her bio, tweets, and follower/following counts.
- Google+:** A profile page for "Roger Federer" showing his photo, bio, and a link to his Google+ page.

Below the screenshots is a copyright notice: "Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited."



People Search on Social Networking Services

Searching for people on social networking websites is easy. Social networking services are the online services, platforms, or sites that focus on facilitating the building of social networks or social relations among people. These websites provide information that is provided by users. Here, people are directly or indirectly related to each other by **common interest**, work location, or educational communities, etc.

Social networking sites allow people to share information quickly and effectively as these sites are updated in real time. It allows updating facts about upcoming or current events, recent announcements and invitations, and so on. Therefore, social networking sites prove to be a great platform for searching people and their related information. Through people searching on **social networking services**, you can gather critical information that will be helpful in performing social engineering or other kinds of attacks.

Many social networking sites allow visitors to search for people without registration; this makes people searching on social networking sites an easy task for you. You can search a person using name, email, or address. Some sites allow you to check whether an account is currently in use or not. This allows you to check the status of the person you are looking for.

Some of social networking services are as follows:



Facebook

Source: <http://www.facebook.com>

Facebook allows you to search for people, their **friends**, **colleagues**, and **people** living around them and others with whom they are affiliated. In addition, you can also find their professional information such as their company or business, current location, phone number, email ID, photos, videos, etc. It allows you to search for people by username or email address.

FIGURE 2.7: Facebook a social networking service to search for people across the world



LinkedIn

Source: <http://www.linkedin.com>

LinkedIn is a **social networking website** for professional people. It allows you to find people by name, keyword, company, school, etc. Searching for people on LinkedIn gives you information such as name, designation, name of company, current location, and education qualifications, but to use LinkedIn you need to be registered with the site.

FIGURE 2.8: LinkedIn screenshot



Twitter

Source: <http://twitter.com>

Twitter is a social networking service that allows people to send and **read text messages** (tweets). Even unregistered users can read tweets on this site.



FIGURE 2.9: Twitter screenshot

Google+

Source: <https://plus.google.com>

Google+ is a social networking site that aims to make sharing on the web more like **sharing in real life**. You can grab a lot of useful information about users from this site and use it to hack their systems.

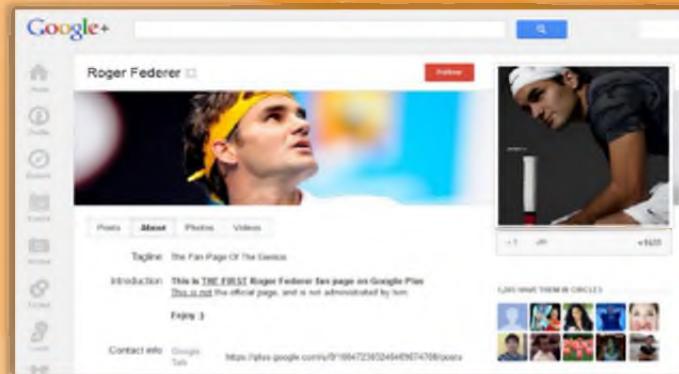


FIGURE 2.10: Google+ screenshot

Gather Information from Financial Services

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



Gather Information from Financial Services

Financial services such as Google Finance, Yahoo! Finance, and so on provide a lot of useful information such as the market value of a company's shares, company profile, competitor details, etc. The information offered varies from one service to the next. In order to avail themselves of services such as e-mail alerts and phone alerts, users need to register on the financial services. This gives an opportunity for an attacker to **grab useful information for hacking**.

Many financial firms rely on web access, performing transactions, and user access to their accounts. Attackers can obtain sensitive and private information of users using information theft, key loggers, etc. Attackers can even grab this information by implementing cybercrimes, and exploit it with the help of non-vulnerable threats (software design flaw example; breaking authentication mechanism).

The following are some of non-vulnerable threats:

- ⌚ Service flooding
- ⌚ Brute force attack
- ⌚ Phishing

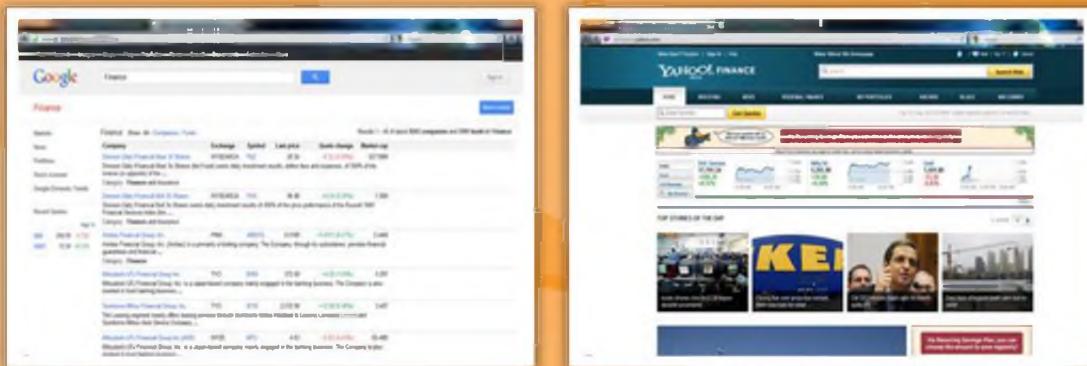


FIGURE 2.11: Examples of financial services website for gathering information

Footprinting through Job Sites



You can gather **company's infrastructure details** from job postings

Look for these:

- Job requirements
- Employee's profile
- Hardware information
- Software information

Examples of Job Websites

- <http://www.monster.com>
- <http://www.careerbuilder.com>
- <http://www.dice.com>
- <http://www.simplyhired.com>
- <http://www.indeed.com>
- <http://www.usajobs.gov>

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



Footprinting through Job Sites

Attackers can gather valuable information about the operating system, software versions, company's infrastructure details, and **database schema** of an organization, through footprinting various job sites using different techniques. Depending upon the posted requirements for job openings, attackers may be able to study the hardware, network-related information, and technologies used by the company. Most of the company's websites have a key employees list with their email addresses. This information may prove to be beneficial for an attacker. For example, if a company wants to hire a person for a **Network Administration job**, it posts the requirements related to that position.

Enterprise Applications Engineer@BIA

Job Description:

The Enterprise Applications Engineer's role is to plan, implement, manage, administer and support core business application software for corporate enterprise needs. This includes, but is not limited to: Microsoft IIS, Microsoft Exchange 2010, Microsoft SharePoint, Microsoft Project Server, Microsoft Project, Microsoft CRM, Microsoft SQL, Service Pack 2008, Microsoft Team Foundation Server 2008 and 2010, Microsoft SCOM, proprietary developed software and open source applications utilized by the company.

Job Knowledge and Skills:

Position requires strong knowledge of Windows server 2008/2005 Active Directory administration and networking (TCP/IP, DNS and DHCP). Must have experience with and strong working knowledge of Microsoft SQL 2008 and 2005, Microsoft Exchange 2010 messaging systems, Microsoft SharePoint, Microsoft Project, Microsoft CRM and SCOM. Must have basic programming and scripting skills. Proficient with Microsoft Shell interface (CMD). Must be knowledgeable of server hardware and Network Infrastructure best practices. MCITP EA, server messaging, SQL, and/or MCTS, MCSE certification preferred. Bachelor degree in Computer Science or Network Engineering, professional training or equivalent experience.

POSITION INFORMATION

Job ID: 17123 6554870 6
Location: Boca Raton, FL 33487

Job Status: IT/Software Development

Industry: Insurance

Work Experience: 5+ to 7 Years

Career Level: Experienced (Ex-Manager)

Education Level: Postsecondary

CONTACT INFORMATION

Job Description:

Design and implement technical solutions on the Windows platform to support business requirements.

Support existing Windows infrastructure including Active Directory 2003, SBS, BUB, Cowa Metaphase, SQL Server, SQL Clusters, Exchange 5.5, Exchange 2003, VM Ware, Veritas backup software, Account and server security, Disaster Recovery services, RAID technologies, and FibreSAN disk solutions.

Job Experience:

- 5 or more years experience working in IT implementing and supporting a global business
- Prior experience in supporting a global Windows server and Domain infrastructure
- Experience implementing and supporting Active Directory, Cowa Metaphase, SQL Server, SQL Cluster, DNS, DHCP, WINS, and Exchange 2003 in an Enterprise environment
- Very strong system troubleshooting skills
- Experience in providing 24-hour support to a global enterprise as part of an on-call rotation
- Effective interpersonal skills with the ability to be persuasive
- Other skills: Building Effective Teams, Action Oriented Peer Relationships, Customer Focus, Priority Setting, Problem Solving, and Business Acumen
- Bachelor's Degree or equivalent experience
- MCSE (2003) certification a plus, Cisco Certification a plus

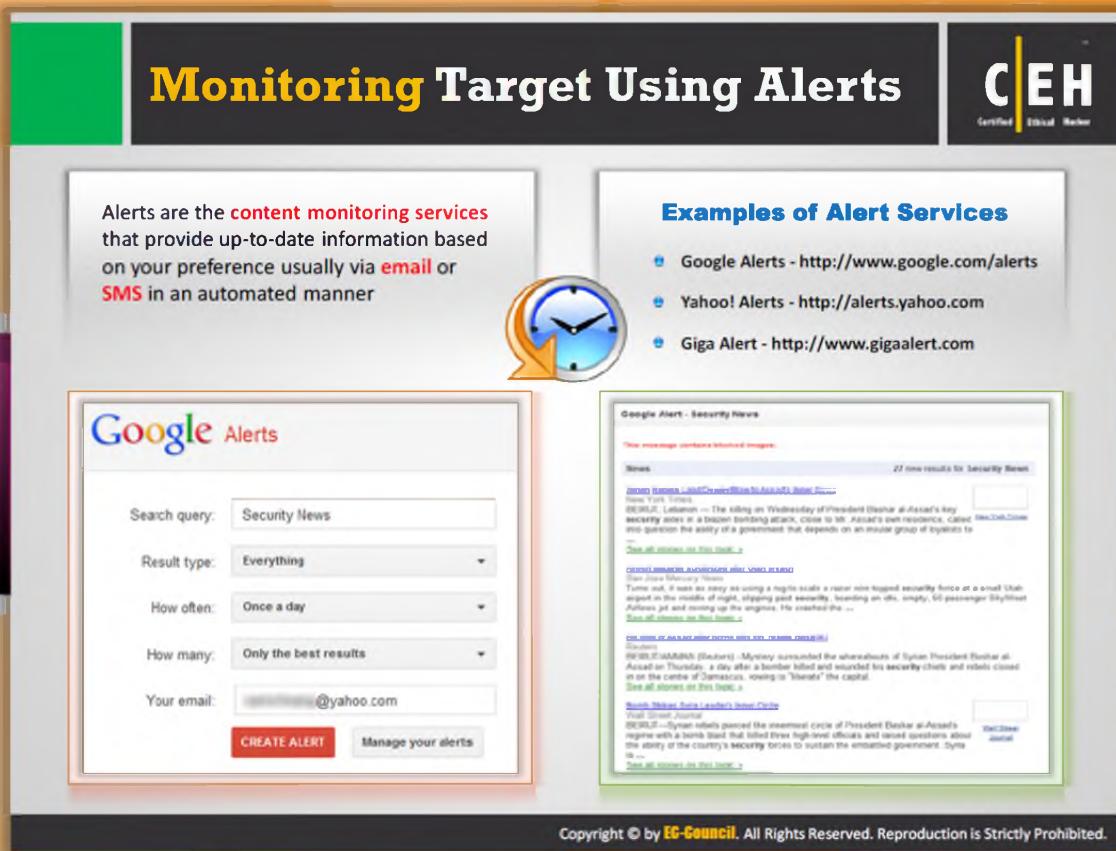
FIGURE 2.12: Gathering information through Job websites

Usually attackers look for the following information:

- Job requirements
- Employee's profile
- Hardware information
- Software information

Examples of job websites include:

- <http://www.monster.com>
- <http://www.careerbuilder.com>
- <http://www.dice.com>
- <http://www.simplyhired.com>
- <http://www.indeed.com>
- <http://www.usajobs.gov>



The slide has a green header bar with the title "Monitoring Target Using Alerts". In the top right corner is the CEH logo. The main content area contains two sections: "Alerts are the content monitoring services that provide up-to-date information based on your preference usually via email or SMS in an automated manner" with a clock icon, and "Examples of Alert Services" listing Google Alerts, Yahoo! Alerts, and Giga Alert. Below these are screenshots of the Google Alerts interface and a search results page for "Security News". The footer of the slide includes the copyright notice "Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited."

Alerts are the **content monitoring services** that provide up-to-date information based on your preference usually via **email** or **SMS** in an automated manner

Examples of Alert Services

- Google Alerts - <http://www.google.com/alerts>
- Yahoo! Alerts - <http://alerts.yahoo.com>
- Giga Alert - <http://www.gigaalert.com>

Google Alerts

Search query: Security News
Result type: Everything
How often: Once a day
How many: Only the best results
Your email: [redacted]@yahoo.com
CREATE ALERT Manage your alerts

Google Alert - Security News

27 news results for Security News

SYRIA: Syria's security forces have arrested a man who reportedly shot dead a member of the opposition Free Syrian Army (FSA) in the town of Idlib, killing four people. The man was reportedly carrying a bomb vest and was shot dead by FSA fighters during a clash between them and security forces in the town of Idlib.

SYRIA: A car bomb exploded in the center of Damascus, killing at least 10 people and wounding 20 others. The explosion occurred near the residence of President Bashar al-Assad on Thursday, a day after a suicide bombing killed three officials and wounded his security chief and rebels claimed it was carried out by the Islamic State group.

SYRIA: A car bomb exploded in the center of Damascus, killing at least 10 people and wounding 20 others. The explosion occurred near the residence of President Bashar al-Assad on Thursday, a day after a suicide bombing killed three officials and wounded his security chief and rebels claimed it was carried out by the Islamic State group.

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



Monitoring Targets Using Alerts

Alerts are the content monitoring services that provide automated up-to-date information based on your preference, usually via **email** or **SMS**. In order to get alerts, you need to register on the website and you should submit either an email or phone number to the service. Attackers can gather this sensitive information from the **alert services** and use it for further processing of an attack.



Google Alerts

Source: <http://www.google.com/alerts>

Google Alerts is a content monitoring service that automatically notifies users when new content from news, web, blogs, video, and/or discussion groups matches a set of search terms selected by the user and stored by the Google Alerts service.

Google Alerts aids in monitoring a developing news story and keeping current on a **competitor** or **industry**.

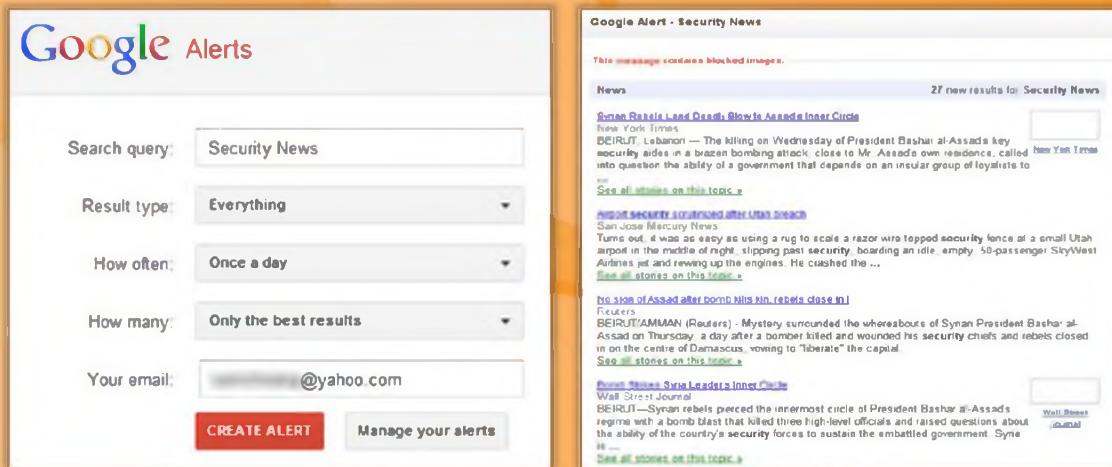


FIGURE 2.13: Google Alert services screenshot

Yahoo! Alerts is available at <http://alerts.yahoo.com> and Giga Alert is available at <http://www.gigaalert.com>; these are two more examples of alert services.



Footprinting Methodology

So far, we have discussed the first step of footprinting methodology, i.e., footprinting via search engines. Now we will discuss website footprinting. An **organization's website** is a first place where you can get sensitive information such as names and contact details of chief persons in the company, upcoming project details, and so on. This section covers the website footprinting concept, mirroring websites, the tools used for mirroring, and **monitoring web updates**.

Website Footprinting

Information obtained from target's website enables an attacker to build a detailed **map of website's structure and architecture**

Browsing the target website may provide:

- Software used and its version
- Operating system used
- Sub-directories and parameters
- Filename, path, database field name, or query
- Scripting platform
- Contact details and CMS details

Use Zaproxy, Burp Suite, Firebug, etc. to view headers that provide:

- Connection status and content-type
- Accept-Ranges
- Last-Modified information
- X-Powered-By information
- Web server in use and its version

Screenshot of Burp Suite:

The screenshot shows the Burp Suite interface with a list of captured requests and responses. One request is highlighted in green, showing a response for a file named 'index.php'. The response pane displays the raw HTTP response, which includes the following header:

```
HTTP/1.1 200 OK
Date: Fri, 10 Jul 2015 08:00:00 GMT
Content-Type: application/x-javascript
Content-Length: 794
Last-Modified: Fri, 10 Jul 2015 08:00:00 GMT
ETag: "48d-1000000000000000"
Server: Apache/2.4.10 (Ubuntu)
X-Powered-By: PHP/5.6.28-0ubuntu0.15.04.1
```

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



Website Footprinting

It is possible for an attacker to build a detailed map of a website's structure and architecture without IDS being triggered or without raising any sys admin suspicions. It can be accomplished either with the help of sophisticated footprinting tools or just with the basic tools that come along with the operating system, such as **telnet** and a **browser**.

Using the **Netcraft tool** you can gather website information such as IP address, registered name and address of the domain owner, domain name, host of the site, OS details, etc. But this tool may not give all these details for every site. In such cases, you should browse the target website.

Browsing the target website will provide you with the following information:

- Software used and its version: You can find not only the software in use but also the version easily on the off-the-shelf **software-based** website.
- Operating system used: Usually the operating system can also be determined.
- Sub-directories and parameters: You can reveal the **sub-directories** and parameters by making a note of all the URLs while browsing the target website.

- ➊ Filename, path, database field name, or query: You should analyze anything after a query that looks like a filename, path, database field name, or query carefully to check whether it offers opportunities for SQL injection.
- ➋ Scripting platform: With the help of the script filename extensions such as .php, .asp, .jsp, etc. you can easily determine the scripting platform that the target website is using.
- ➌ Contact details and CMS details: The contact pages usually offer details such as names, phone numbers, email addresses, and locations of admin or support people. You can use these details to perform a social engineering attack.

CMS software allows URL rewriting in order to disguise the script filename extensions. In this case, you need to put little more effort to determine the scripting platform.

Use Paros Proxy, Burp Suite, Firebug, etc. to view headers that provide:

- ➊ Connection status and content-type
- ➋ Accept-ranges
- ➌ Last-Modified information
- ➍ X-Powered-By information
- ➎ Web server in use and its version

Source: <http://portswigger.net>

The following is a screenshot of Burp Suite showing headers of packets in the information pane:

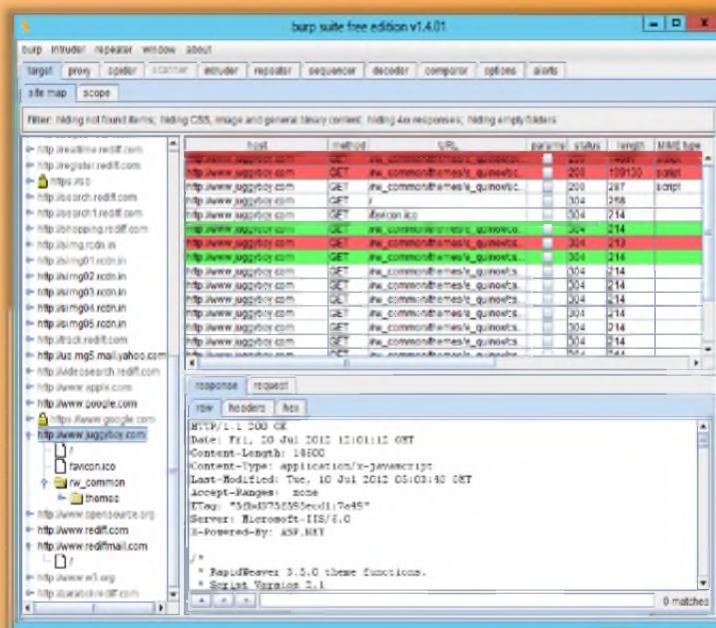
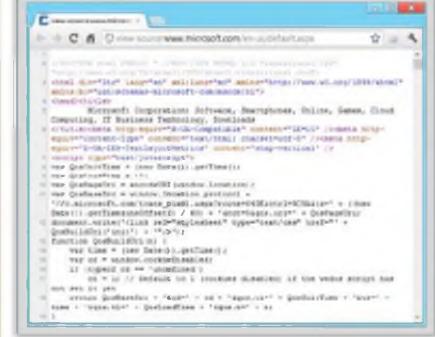


FIGURE 2.14: Burp Suite showing headers of packets in the information pane

Website Footprinting (Cont'd)

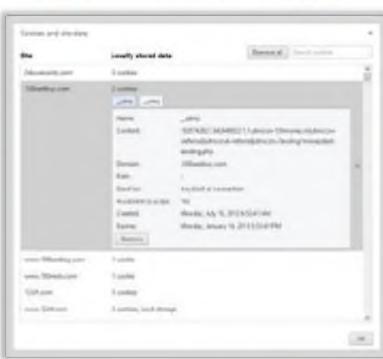
Examining HTML source provides:

- Comments in the source code
- Contact details of web developer or admin
- File system structure
- Script type



Examining cookies may provide:

- Software in use and its behavior
- Scripting platforms used



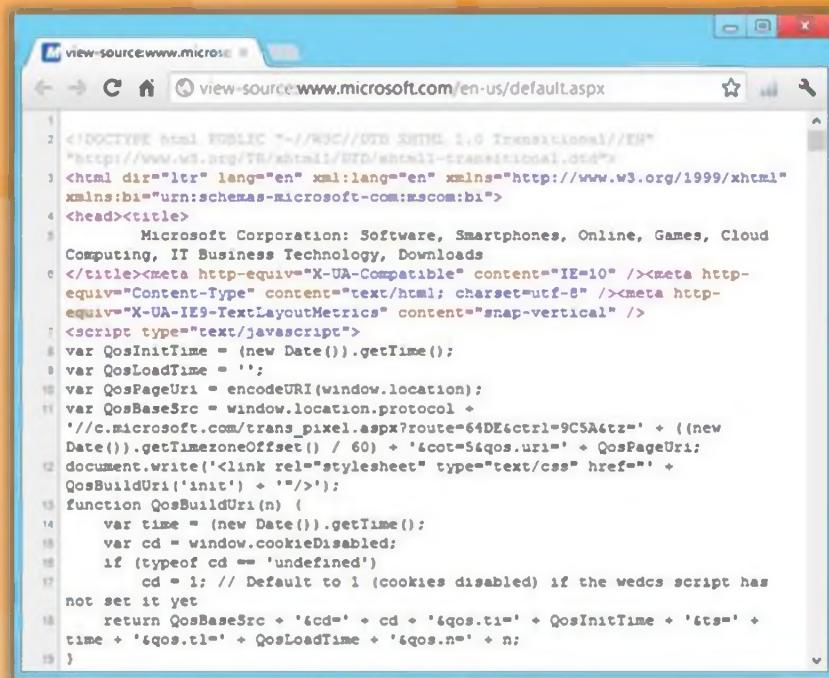
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



Website Footprinting (Cont'd)

Examine the **HTML source code**. Follow the comments that are either created by the CMS system or inserted manually. These comments may provide clues to help you understand what's running in the background. This may even provide contact details of the web admin or developer.

Observe all the links and image tags, in order to map the file system structure. This allows you to reveal the existence of hidden directories and files. Enter **fake data** to determine how the script works.



The screenshot shows the source code of a Microsoft page. The code includes various meta tags, a title, and a script section. The script handles cookie management, specifically setting a cookie named '_utmc' with a value of '192874282.1342446822.1.1.utmcsrc=100money.injutmccn&(referral)utmcrnd=referal|utmccnx:/landing/moneydeal-lending.php'. It also checks for cookie disabled status and sets a default value of 1 if cookies are disabled.

```
<!--><!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0 Transitional//EN"
 "http://www.w3.org/TR/ht/html2/HTML/htmll-transitional.dtd">
<html dir="ltr" lang="en" xml:lang="en" xmlns="http://www.w3.org/1999/xhtml"
 xmlns:bi="urn:schemas-microsoft-com:mscom:bi">
<head><title>
    Microsoft Corporation: Software, Smartphones, Online, Games, Cloud
    Computing, IT Business Technology, Downloads
</title><meta http-equiv="X-UA-Compatible" content="IE=10" /><meta http-
equiv="Content-Type" content="text/html; charset=utf-8" /><meta http-
equiv="X-UA-IE9-TextLayoutMetrics" content="snap-vertical" />
<script type="text/javascript">
var QosInitTime = (new Date()).getTime();
var QosLoadTime = '';
var QosPageUri = encodeURI(window.location);
var QosBaseSrc = window.location.protocol +
    '//c.microsoft.com/trans_pixel.aspx?route=64DE6ctrl=9C5A6tz=' + ((new
Date()).getTimezoneOffset() / 60) + '&cot=5iqos.uri=' + QosPageUri;
document.write('<link rel="stylesheet" type="text/css" href="' +
QosBuildUri('init') + '">');
function QosBuildUri(n) {
    var time = (new Date()).getTime();
    var cd = window.cookieDisabled;
    if (typeof cd == 'undefined')
        cd = 1; // Default to 1 (cookies disabled) if the wedcs script has
not set it yet
    return QosBaseSrc + '&cd=' + cd + '&qos.ti=' + QosInitTime + '&ts=' +
time + '&qos.tl=' + QosLoadTime + '&qos.n=' + n;
}
</script>
```

FIGURE 2.15: Screenshot showing Microsoft script works

Examine cookies set by the server to determine the software running and its behavior. You can also identify the script in platforms by observing sessions and other supporting **cookies**.

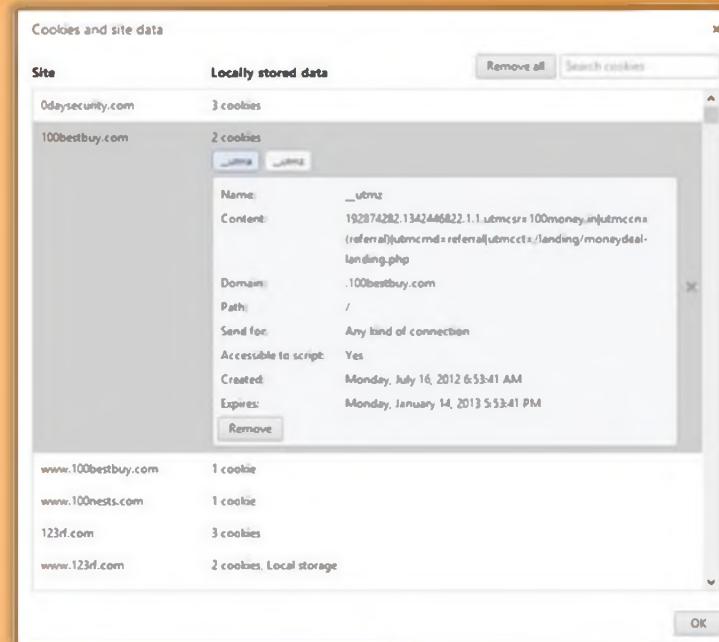


FIGURE 2.16: Showing details about the software running in a system by examining cookies

Mirroring Entire Website

C|EH
Certified Ethical Hacker

- Mirroring an entire website onto the local system enables an attacker to **dissect and identify vulnerabilities**; it also assists in finding **directory structure** and other valuable information without multiple requests to web server
- Web mirroring tools allow you to **download a website to a local directory**, building recursively all directories, HTML, images, flash, videos, and other files from the server to your computer

Original Website Mirrored Website

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



Mirroring an Entire Website

Website mirroring is the process of creating an exact replica of the original website. This can be done with the help of web mirroring tools. These tools allow you to download a website to a local directory, recursively building all **directories, HTML, images, flash, videos** and other files from the server to your computer.

Website mirroring has the following benefits:

- It is helpful for offline site browsing.
- Website mirroring helps in creating a backup site for the original one.
- A website clone can be created.
- Website mirroring is useful to test the site at the time of website design and development.
- It is possible to distribute to **multiple servers** instead of using only one server.



FIGURE 2.17: JuggyBoy's Original and Mirrored website

Website Mirroring Tools

The collage displays four software interfaces for website mirroring:

- HTTrack Web Site Copier** (<http://www.httrack.com>): A Windows application showing a file tree and download progress.
- BlackWidow** (<http://softbytelabs.com>): A web browser interface showing a mirrored Microsoft homepage.
- SurfOffline** (<http://www.surffoffline.com>): A Windows application showing a list of files and download status.
- WebRipper** (<http://www.calluna-software.com>): A web browser interface showing a mirrored JuggboyQuestion the Rules page.

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

Website Mirroring Tools



HTTrack Web Site Copier

Source: <http://www.httrack.com>

HTTrack is an offline browser utility. It allows you to download a World Wide Web site from the Internet to a **local directory**, building recursively all directories, getting HTML, images, and other files from the server to your computer. HTTrack arranges the original **site's relative link-structure**. Open a page of the "mirrored" website in your browser, browse the site from link to link, and you can view the site as if you were online. HTTrack can also update an existing mirrored site, and resume interrupted downloads.

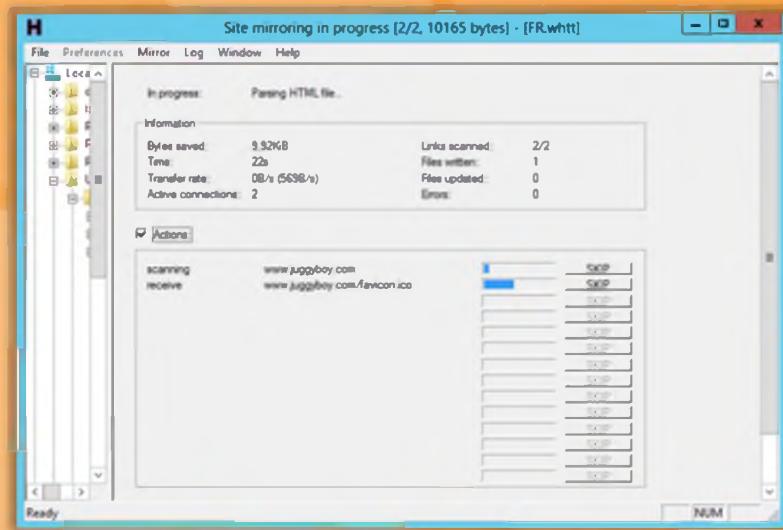


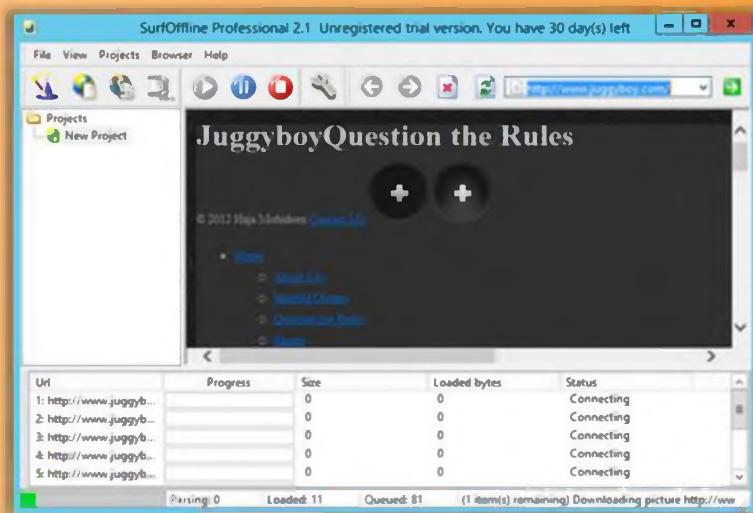
FIGURE 2.18: HTTrack Web Site Copier Screenshot



SurfOffline

Source: <http://www.surfoffline.com>

SurfOffline is a website download **software**. The software allows you to download entire websites and download web pages to your local hard drive. After downloading the target website, you can use SurfOffline as an offline browser and view downloaded web pages in it. If you prefer to view downloaded webpages in another browser, you can use the **Export Wizard**. SurfOffline's Export Wizard also allows you to copy downloaded websites to other computers in order to view them later and prepares websites for burning them to a CD or DVD.



Url	Progress	Size	Loaded bytes	Status
1: http://www.juggyb...	0	0	0	Connecting
2: http://www.juggyb...	0	0	0	Connecting
3: http://www.juggyb...	0	0	0	Connecting
4: http://www.juggyb...	0	0	0	Connecting
5: http://www.juggyb...	0	0	0	Connecting

FIGURE 2.19: SurfOffline screenshot



BlackWidow

Source: <http://softbytelabs.com>

BlackWidow is a website scanner for both experts and beginners. It scans websites (it's a site ripper). It can download an entire website or part of a website. It will build a site structure first, and then downloads. It allows you to choose what to download from the website.



FIGURE 2.20: SurfOffline screenshot



Webripper

Source: <http://www.calluna-software.com>

WebRipper is an Internet scanner and downloader. It downloads massive amount of images, videos, audio, and executable documents from any website. WebRipper uses **spider-technology** to follow the links in all directions from the start-address. It filters out the interesting files, and adds them to the download-queue for downloading.

You can restrict downloaded items by file type, minimum file, maximum file, and image size. All the downloaded links can also be restricted by keywords to avoid wasting your **bandwidth**.

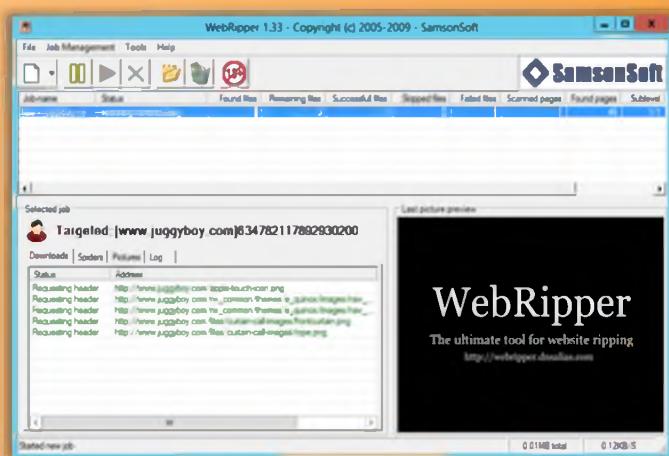


FIGURE 2.21: Webripper screenshot

Website Mirroring Tools (Cont'd)



The slide displays a grid of nine website mirroring tools, each with an icon and a link to its website. The tools are:

- Website Ripper Copier** (<http://www.tensors.com>)
- PageNest** (<http://www.pagenest.com>)
- Teleport Pro** (<http://www.tenmax.com>)
- Backstreet Browser** (<http://www.spadixbd.com>)
- Portable Offline Browser** (<http://www.metaproducts.com>)
- Offline Explorer Enterprise** (<http://www.metaproducts.com>)
- Proxy Offline Browser** (<http://www.proxy-offline-browser.com>)
- GNU Wget** (<http://www.gnu.org>)
- iMiser** (<http://internetresearchtool.com>)
- Hooeey Webprint** (<http://www.hooeeywebprint.com>)

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



Website Mirroring Tools (Cont'd)

In addition to the website mirroring tools mentioned previously, a few more well-known tools are mentioned as follows:

- ⌚ Website Ripper Copier available at <http://www.tensors.com>
- ⌚ Teleport Pro available at <http://www.tenmax.com>
- ⌚ Portable Offline Browser available at <http://www.metaproducts.com>
- ⌚ Proxy Offline Browser available at <http://www.proxy-offline-browser.com>
- ⌚ iMiser available at <http://internetresearchtool.com>
- ⌚ PageNest available at <http://www.pagenest.com>
- ⌚ Backstreet Browser available at <http://www.spadixbd.com>
- ⌚ Offline Explorer Enterprise available at <http://www.metaproducts.com>
- ⌚ GNU Wget available at <http://www.gnu.org>
- ⌚ Hooeey Webprint available at <http://www.hooeeywebprint.com>

Extract Website Information from <http://www.archive.org>

Internet Archive's Wayback Machine allows you to visit **archived versions of websites**



A screenshot of a computer window showing the Internet Archive Wayback Machine interface. The URL in the address bar is <http://wayback.archive.org/wayback/help/microsoft.com>. The page displays a timeline of archived versions of the Microsoft website from January 2001 to August 2011. The timeline shows a dense grid of dates with many entries highlighted in blue, indicating available archive versions. A large watermark for 'Wayback Machine' is visible across the timeline area.

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



Extract Website Information from <http://www.archive.org>

Archive is an **Internet Archive Wayback Machine** that allows you to visit archived versions of websites. This allows you to gather information on a company's web pages since their creation. As the website www.archive.org keeps track of web pages from the time of their inception, you can retrieve even information that has been removed from the **target website**.

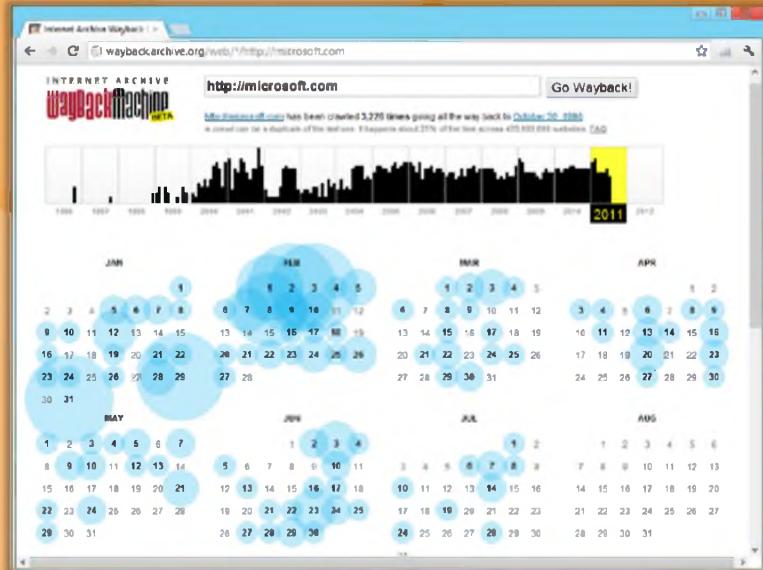


FIGURE 2.22: Internet Archive Wayback Machine screenshot

The screenshot shows the WEBSITE-WATCHER 2012 (1.2.2) application window. The main area displays a list of monitored websites with columns for Name, URL, Last change, Status, and Last check. A red ribbon highlights the 'Bookmarks' section on the left. Below the list is a browser window showing the 'WebSite-Watcher' homepage with a download link for 'WebSite-Watcher 4.4.2'. The URL <http://aigues.com> is visible at the bottom right of the browser window.



Monitoring Web Updates Using Website Watcher

Source: <http://www.aignes.com>

Website Watcher is used to keep track of websites for updates and automatic changes. When an update or change occurs, Website Watcher automatically detects and saves the last two versions onto your disk, and highlights changes in the text. It is a useful tool for monitoring sites to gain **competitive advantage**.

Benefits:

Frequent manual checking of updates is not required. Website Watcher can automatically detect and notify users of updates:

- ⌚ It allows you to know what your competitors are doing by scanning your competitors' websites
- ⌚ The site can keep track of new software versions or driver updates
- ⌚ It stores images of the modified websites to a **disk**

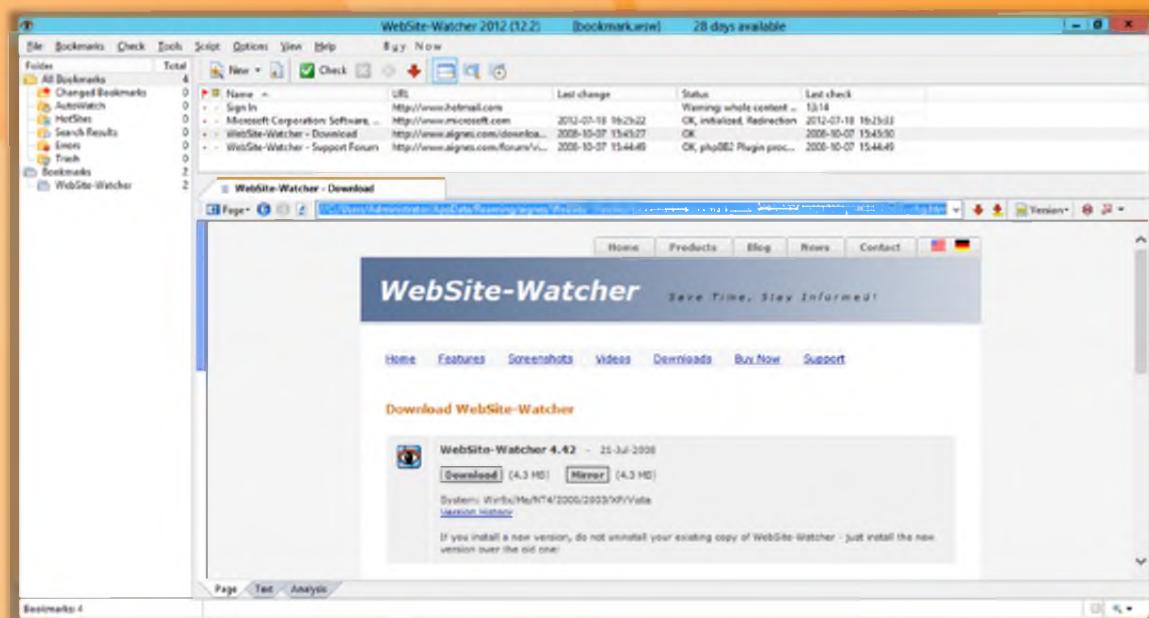


FIGURE 2.23: Website watcher monitoring web updates



Footprinting Methodology

So far we have discussed Footprinting through search engines and website footprinting, the two initial phases of footprinting methodology. Now we will discuss **email footprinting**.



This section describes how to track email communications, how to collect information from email headers, and email tracking tools.

Tracking Email Communications

CEH
Certified Ethical Hacker

- Attacker tracks email to gather information about the **physical location of an individual** to perform social engineering that in turn may help in **mapping target organization's network**
- Email tracking is a method to **monitor and spy on the delivered emails** to the intended recipient

The diagram shows a central circle divided into six segments, each containing a piece of information that can be tracked:

- When the email was received and read
- GPS location and map of the recipient
- Time spent on reading the emails
- Whether or not the recipient visited any links sent to them
- Track PDF and other types of attachments
- Set messages to expire after a specified time

Icons around the circle represent different tracking categories: a telephone and envelope icon for communication, a magnifying glass over a map for location, a clock for time spent, a PDF icon for attachments, and a gear icon for settings.

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



Tracking Email Communications

Email tracking is a method that helps you to monitor as well as to track the emails of a particular user. This kind of tracking is possible through digitally time stamped records to reveal the time and date a particular email was received or opened by the target. A lot of email **tracking tools** are readily available in the market, using which you can collect information such as IP addresses, mail servers, and service provider from which the mail was sent. Attackers can use this information to build the **hacking strategy**. Examples of email tracking tools include: eMailTrackerPro and Paraben E-mail Examiner.

By using email tracking tools you can gather the following information about the victim:

- Geolocation:** Estimates and displays the location of the recipient on the map and may even calculate distance from your location.
- Read duration:** The duration of time spent by the recipient on reading the mail sent by the sender.
- Proxy detection:** Provides information about the type of server used by the recipient.
- Links:** Allows you to check whether the links sent to the recipient through email have been checked or not.

- ➊ **Operating system:** This reveals information about the type of operating system used by the recipient. The attacker can use this information to launch an attack by finding loopholes in that particular operating system.
- ➋ **Forward email:** Whether or not the email sent to you is forwarded to another person can be determined easily by using this tool.

Collecting Information from Email Header

The screenshot shows a sample email header with several fields annotated:

- Delivered-To:** [redacted] @gmail.com
- Received:** by 10.112.39.167 with SMTP id q7ca...
Fri, 1 Jun 2012 21:24:01 -0700 (PDT)
- Return-Path:** <[redacted]@gmail.com>
- Received-SPF:** pass (google.com: domain of [redacted] designates 10.224.205.137 as permitted sender) client-ip=10.224.205.137;
- Authentication-Results:** mr.google.com; dkim=pass header.i=[redacted]@gmail.com
- Received:** from mr.google.com ([10.224.205.137])
by 10.224.205.137 with SMTP id fq9m=578570qab.39.13
Fri, 01 Jun 2012 21:24:00 -0700 (PDT)
- DKIM-Signature:** v=1; a=rsa-sha256; c=relaxed/relaxed;
d=gmail.com; s=20120113;
h=mime-version:in-reply-to:references:content-type:
b=TGE1Bb4ti7gQG4gh7okpjxw+Tt/iAC1
b=KguZLTLfq2+QZxjZKex1NnvRcND/+P4+Nk
b=PK3eJ3Uf/CsaBZWDIT0X1aKOAGR3BOT92MC2FxeUUQ9uwL/xHALSnk2UTFFeKGqOC
o=9hD59D3oxI6KA7Zmkb1GzXmV4DIWffCL894RaMBQOoMzRwOWNI1b95a1I38cqtlfP
ZhrWFKh5xNzKsR73x2PFYzp7yecC=QuYHZNGs1Kxc07xQj@Zuw+HWR/vk6xChDJap24
K5ZAFYzmkkPK+VdL2qu7YGFzy6oHcuPl6y3/C2fXHVdsuYamNT/yevvhCvo8Og7FRt6
/Kzw=
- MIME-Version:** 1.0
- Received:** by 10.224.205.137 with SMTP id fq9m=704562c...; Fri, 01 Jun 2012 21:24:00 -0700 (PDT)
- Received:** by 10.229.230.79 with HTTP; Fri, 1 Jun 2012 21:24:00 -0700 (PDT)
- In-Reply-To:** <CAOYWATT1zDXE3o8D2ihxE4BerZM...>
- References:** <CAOYWATT1zDXE3o8D2ihxE4BerZM...>
- Date:** Fri, 01 Jun 2012 21:24:00 +0000
- Message-ID:** <CASevxi0qe1nfwu-d1Qhno-EMJcgfgX+mUfjB_tt2ay2dXA@mail.gmail.com>
- Subject:** Re: [REDACTED] SOLUTIONS !!!
- From:** [redacted] Mirra <[redacted]@gmail.com>
- To:** [redacted]@gmail.com, [redacted]@gmail.com, [redacted]@yahoo.com, [redacted]@yahoo.com

Annotations explain the following fields:

- Sender's IP address:** 10.224.205.137
- The address from which the message was sent:** [redacted]@gmail.com
- Sender's mail server:** mr.google.com
- Date and time received by the originator's email servers:** Fri, 01 Jun 2012 21:24:00 -0700 (PDT)
- Authentication system used by sender's mail server:** DKIM
- A unique number assigned by mr.google.com to identify the message:** 1040318
- Sender's full name:** Mirra

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



Collecting Information from Email Headers

An email header is the information that travels with every email. It contains the details of the sender, routing information, date, subject, and recipient. The process of viewing the **email header** varies with different mail programs.

Commonly used email programs:

- ⌚ SmarterMail Webmail
- ⌚ Outlook Express 4-6
- ⌚ Outlook 2000-2003
- ⌚ Outlook 2007
- ⌚ Eudora 4.3/5.0
- ⌚ Entourage
- ⌚ Netscape Messenger 4.7
- ⌚ MacMail

The following is a screenshot of a sample email header.

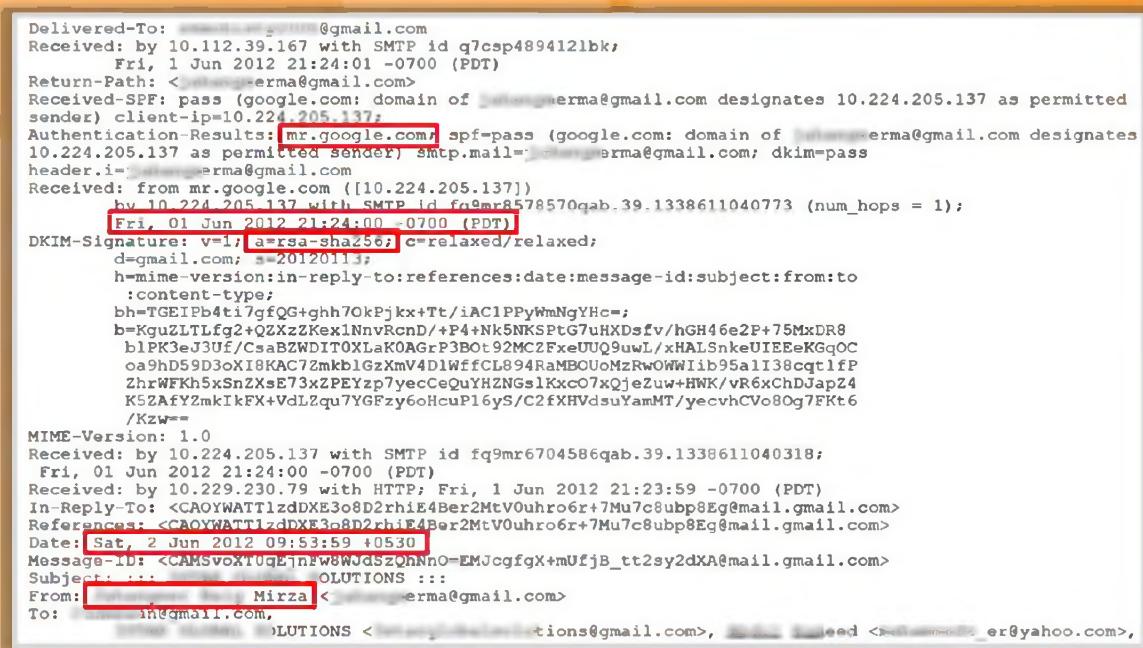


FIGURE 2.24: Email header screenshot

This email header contains the following information:

- Sender's mail server
 - Data and time received by the originator's email servers
 - Authentication system used by sender's mail server
 - Data and time of message sent
 - A unique number assigned by mr.google.com to identify the message
 - Sender's full name
 - Senders IP address
 - The address from which the message was sent

The attacker can trace and collect all of this information by performing a detailed analysis of the complete [email header](#).

Email Tracking Tools

The screenshot displays three email tracking tools:

- eMailTrackerPro** (<http://www.emailtrackerpro.com>): A Windows application interface showing a world map and a list of tracked emails.
- PoliteMail** (<http://www.politemail.com>): A web-based interface showing email metrics and a bar chart.
- Email Lookup - Free Email Tracker** (<http://www.ipaddresslocation.org>): A web-based tool showing an IP header analysis and a map of Lansing, Michigan.

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



Email Tracking Tools

Email tracking tools allow you to track an email and extract information such as **sender identity**, **mail server**, **sender's IP address**, etc. You can use the extracted information to attack the target organization's systems by sending malicious emails. Numerous email tracking tools are readily available in the market.

The following are a few commonly used email tracking tools:



eMailTrackerPro

Source: <http://www.emailtrackerpro.com>

eMailTrackerPro is an email tracking tool that analyzes email headers and reveals information such as sender's geographical location, IP address, etc. It allows you to review the traces later by saving all past traces.



FIGURE 2.25: eMailTrackerPro showing geographical location of sender



PoliteMail

Source: <http://www.politemail.com>

PoliteMail is an email tracking tool for Outlook. It tracks and provides complete details about who opened your mail and which document has been opened, as well as which links are being clicked and read. It offers mail merging, split testing, and full list management including segmenting. You can compose an email containing **malicious links** and send it to the employees of the target organization and keep track of your email. If the employee clicks on the link, he or she is infected and you will be notified. Thus, you can gain control over the system with the help of this tool.

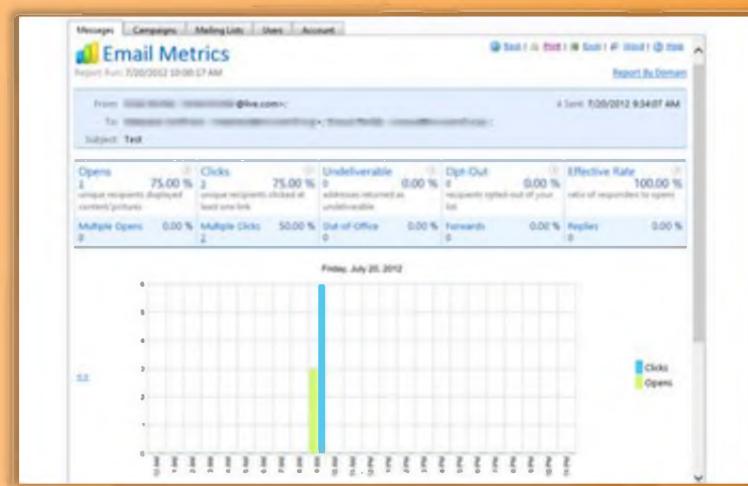


FIGURE 2.26: Politemail screenshot



Email Lookup – Free Email Tracker

Source: <http://www.ipaddresslocation.org>

Email Lookup is an email tracking tool that determines the IP address of the sender by analyzing the **email header**. You can copy and paste the email header into this email tracking tool and start tracing email.

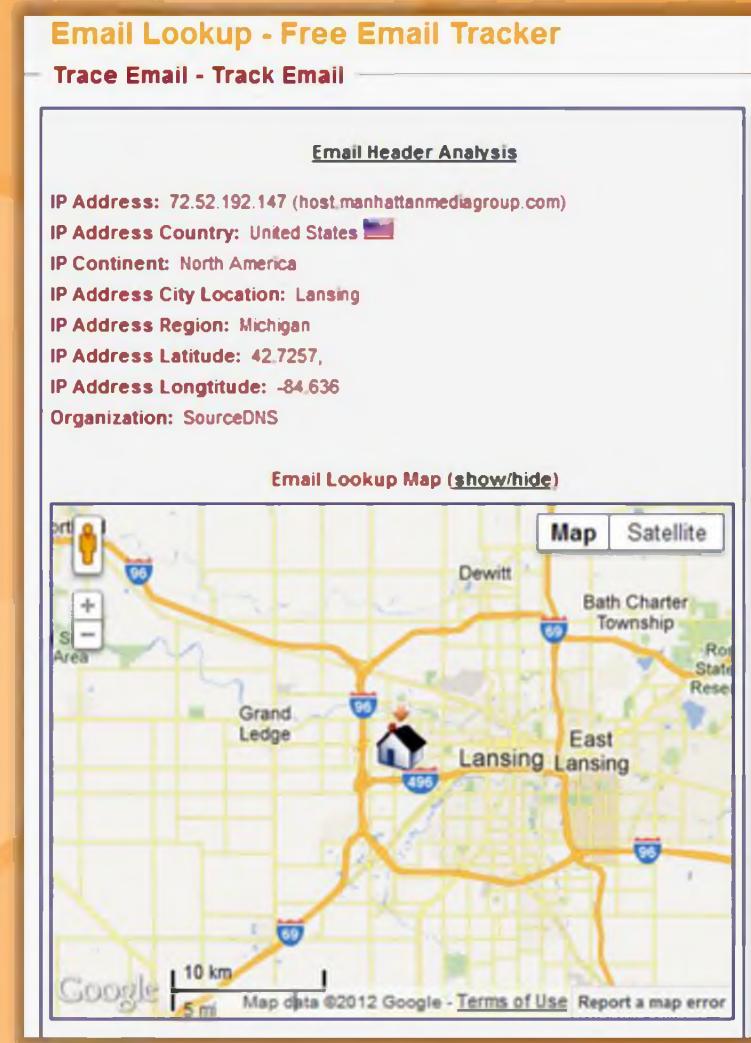


FIGURE 2.27: Email Lookup Screenshot

Email Tracking Tools (Cont'd)

CEH
Certified Ethical Hacker

 Read Notify http://www.readnotify.com	 Pointofmail http://www.pointofmail.com
 DidTheyReadIt http://www.didtheyreadit.com	 Super Email Marketing Software http://www.bulk-email-marketing-software.net
 Trace Email http://whatismyipaddress.com	 WhoReadMe http://whoreadme.com
 MSGTAG http://www.msgtag.com	 GetNotify http://www.getnotify.com
 Zendio http://www zendio com	 G-Lock Analytics http://glockanalytics.com

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

Email Tracking Tools (Cont'd)



Read Notify

Source: <http://www.readnotify.com>

Read Notify provides an email tracking service. It notifies you when a tracked email is opened, re-opened, or forwarded. Read **Notify tracking** reports contain information such as complete delivery details, date and time of opening, geographic location of recipient, visualized map of location, IP address of the recipients, referrer details (i.e., if accessed via web email account etc.), etc.



DidTheyReadIt

Source: <http://www.didtheyreadit.com>

DidTheyReadIt is an email tracking utility. In order to use this utility you need to sign up for an account. Then you need to add ".DidTheyReadIt.com" to the end of the recipient's e-mail address. For example, if you were sending an e-mail to ellen@aol.com, you'd just send it to **ellen@aol.com.DidTheyReadIt.com** instead, and your email would be **tracked**. **ellen@aol.com** would not see that you added .DidTheyReadIt.com to her email address. This utility tracks every email that you send invisibly, without alerting the recipient. If the user opens your mail, then it

informs you when your mail was opened, how long your email remained open, and the geographic location where your email was viewed.



TraceEmail

Source: <http://whatismyipaddress.com>

The TraceEmail tool attempts to locate the source IP address of an email based on the email headers. You just need to copy and paste the full headers of the target email into the Headers box and then click the Get Source button. It shows the **email header analysis** and results.

This Email header analysis tool does not have the ability to detect forged emails headers. These forged email headers are common in malicious email and spam. This tool assumes all mail servers and email clients in the transmission path are trustworthy.



MSGTAG

Source: <http://www.msgtag.com>

MSGTAG is Windows email tracking software that uses a read receipt technology to tell you when your emails are opened and when your emails are actually read. This software adds a **small track** and trace tag that is unique to each email you need delivery confirmation for. When the email is opened an email tracking code is sent to the MSGTAG email tracking system and an email read confirmation is delivered to you. MSGTAG will notify you when the message is read via an emailed confirmation, a pop-up message, or an **SMS text message**.



Zendio

Source: <http://www zendio com>

Zendio, the email tracking software add-in for Outlook, notifies you once your recipient reads the email, so you can follow up, knowing when they read it and if they clicked on any links included in the email.



Pointofmail

Source: <http://www.pointofmail.com>

Pointofmail.com is a proof of receipt and reading service for email. It ensures read receipts, tracks attachments, and lets you modify or delete sent messages. It provides detailed information about the recipient, full history of email reads and forwards, links and attachments tracking, email, and web and SMS text notifications.



Super Email Marketing Software

Source: <http://www.bulk-email-marketing-software.net>

Super Email Marketing Software is a professional and standalone bulk mailer program. It has the ability to send mails to a list of addresses. It supports both text as well as **HTML formatted emails**. All duplicate email addresses are removed automatically by using this application. Each mail is sent individually to the recipient so that the recipient can only see his or her email in the

email header. It saves the email addresses of the successful sent mails as well as the failed mails to a text, CSV, TSV or Microsoft Excel file.



WhoReadMe

Source: <http://whoreadme.com>

WhoReadMe is an email tracking tool. It is completely invisible to recipients. The recipients will have no idea that the emails sent to them are being tracked. The sender is notified every time the recipient opens the mail sent by the sender. It tracks information such as type of operating system and browser used, Active X Controls, CSS version, duration between the mails sent and read time, etc.



GetNotify

Source: <http://www.getnotify.com>

GetNotify is an email tracking tool that sends notifications when the recipient opens and reads the mail. It sends notifications without the knowledge of recipient.



G-Lock Analytics

Source: <http://glockanalytics.com>

G-Lock Analytics is an **email** tracking service. This allows you to know what happens to your emails after they are sent. This tool reports to you how many times the email was printed and forwarded.



Footprinting Methodology

The next phase in footprinting methodology after email footprinting is **competitive intelligence**.

Competitive intelligence is a process that gathers, analyzes, and distributes intelligence about products, customers, competitors, and technologies using the Internet. The information that is gathered can help managers and executives of a company make **strategic decisions**. This section is about competitive intelligence gathering and sources where you can get valuable information.

Competitive Intelligence Gathering

C|EH
Certified Ethical Hacker

- Competitive intelligence is the process of identifying, gathering, analyzing, verifying, and using information about your competitors from resources such as the Internet
- Competitive intelligence is non-interfering and subtle in nature



Sources of Competitive Intelligence

1	Company websites and employment ads	6	Social engineering employees
2	Search engines, Internet, and online databases	7	Product catalogues and retail outlets
3	Press releases and annual reports	8	Analyst and regulatory reports
4	Trade journals, conferences, and newspaper	9	Customer and vendor interviews
5	Patent and trademarks	10	Agents, distributors, and suppliers

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



Competitive Intelligence Gathering

Various tools are readily available in the market for the purpose of competitive intelligence gathering.

Acquisition of information about products, competitors, and technologies of a company using the Internet is defined as competitive intelligence. Competitive intelligence is not just about **analyzing competitors** but also **analyzing their products, customers, suppliers**, etc. that impact the organization. It is non-interfering and subtle in nature compared to the direct intellectual property theft carried out through hacking or industrial espionage. It mainly concentrates on the external business environment. It gathers information ethically and legally instead of gathering it secretly. According to CI professionals, if the intelligence information gathered is not useful, then it is not called intelligence. **Competitive intelligence** is performed for determining:

- What the competitors are doing
- How competitors are positioning their products and services

Sources of Competitive Intelligence:

- Company websites and employment ads
- Search engines, Internet, and online databases

- ⌚ Press releases and annual reports
- ⌚ Trade journals, conferences, and newspapers
- ⌚ Patents and trademarks
- ⌚ Social engineering employees
- ⌚ Product catalogs and retail outlets
- ⌚ Analyst and regulatory reports
- ⌚ Customer and vendor interviews
- ⌚ Agents, distributors, and suppliers

Competitive intelligence can be carried out by either employing people to search for the information or by utilizing a commercial database service, which incurs a lower cost than employing personnel to do the same thing.

Competitive Intelligence - When Did this Company Begin? How Did it Develop?

The diagram features a central circle labeled 'Company'. Surrounding it are four colored circles: red ('When'), yellow ('How'), blue ('Where'), and green ('Who'). Arrows point from each of these four circles to specific questions: 'When did it begin?', 'How did it develop?', 'Where is it located?', and 'Who leads it?'. A dashed line connects the four primary concepts.

Visit These Sites

- 01. EDGAR Database
<http://www.sec.gov/edgar.shtml>
- 02. Hoovers
<http://www.hoovers.com>
- 03. LexisNexis
<http://www.lexisnexis.com>
- 04. Business Wire
<http://www.businesswire.com>

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



Competitive Intelligence - When Did this Company Begin? How Did it Develop?

Gathering competitor documents and records helps improve **productivity** and **profitability** and stimulate the growth. It helps determine the answers to the following:

When did it begin?

Through competitive intelligence, the history of a company can be collected, such as when a particular company was established. Sometimes, crucial information that isn't usually available for others can also be collected.

How did it develop?

It is very beneficial to know about how exactly a particular company has developed. What are the various strategies used by the company? Their advertisement policy, customer relationship management, etc. can be learned.

Who leads it?

This information helps a company learn details of the leading person (decision maker) of the company.

Where is it located?

The location of the company and information related to various branches and their operations can be collected through competitive intelligence.

You can use this information gathered through competitive intelligence to build a hacking strategy.

The following are information resource sites that help users **gain competitive intelligence**.



EDGAR

Source: <http://www.sec.gov/edgar.shtml>

All companies, foreign and domestic, are required to file registration statements, periodic reports, and other forms electronically through EDGAR. Anyone can view the **EDGAR database** freely through the Internet (web or FTP). All the documents that are filed with the commission by public companies may not be available on EDGAR.



Hoovers

Source: <http://www.hoovers.com>

Hoovers is a business research company that provides complete details about companies and industries all over the world. Hoovers provides patented business-related information through Internet, data feeds, wireless devices, and co-branding agreements with other online services. It gives complete information about the organizations, industries, and people that drive the economy and also provide the tools for connecting to the right people, in order for getting business done.



LexisNexis

Source: <http://www.lexisnexis.com>

LexisNexis is a global provider of content-enabled workflow solutions designed specifically for **professionals in the legal, risk management, corporate, government, law enforcement, accounting, and academic markets**. It maintains an electronic database through which you can get legal and public-records related information. Documents and records of legal, news, and business sources are made accessible to customers.



Business Wire

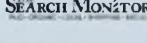
Source: <http://www.businesswire.com>

Business Wire is a company that focuses on press release distribution and regulatory disclosure. Full text news releases, photos, and other multimedia content from thousands of companies and organizations are distributed by this company across the globe to journalists, news media, financial markets, investors, information website, databases, and general audiences. This company has its own patented electronic network through which it releases its news.

Competitive Intelligence - What Are the Company's Plans?



Competitive Intelligence Sites

-  **Market Watch** (<http://www.marketwatch.com>) 
-  **The Wall Street Transcript** (<http://www.twst.com>) 
-  **Lipper Marketplace** (<http://www.lippermarketplace.com>) 
-  **Euromonitor** (<http://www.euromonitor.com>) 
-  **Fagan Finder** (<http://www.faganfinder.com>) 
-  **SEC Info** (<http://www.secinfo.com>) 
-  **The Search Monitor** (<http://www.thesearchmonitor.com>) 

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



Competitive Intelligence - What Are the Company's Plans?

The following are a few more examples of websites that are useful to gather valuable information about various companies and their plans through **competitive intelligence**:



MarketWatch

Source: <http://www.marketwatch.com>

MarketWatch tracks the pulse of markets. The site provides business news, personal finance information, real-time commentary, and investment tools and data, with dedicated journalists generating hundreds of headlines, stories, videos, and market briefs a day.



The Wall Street Transcript

Source: <http://www.twst.com>

The Wall Street Transcript is a website as well as paid subscription publication that publishes industry reports. It expresses the views of money managers and equity analysts of different industry sectors. Interviews with CEOs of companies are published.



Lipper Marketplace

Source: <http://www.lippermarketplace.com>

Lipper Marketplace offers web-based solutions that are helpful for identifying the market of a company. Marketplace helps in qualifying prospects and provides the competitive intelligence needed for transforming these prospects into clients. Its solutions allow users to identify net flows and track institutional trends.



Euromonitor

Source: <http://www.euromonitor.com>

Euromonitor provides strategy research for consumer markets. It publishes reports on industries, consumers, and demographics. It provides market research and surveys focused on your organization's needs.



Fagan Finder

Source: <http://www.faganfinder.com>

Fagan Finder is a collection of internet tools. It is a directory of blog sites, news sites, search engines, photo sharing sites, science and education sites, etc. Specialized tools such as Translation Wizard and URL info are available for finding information about various actions with a web page.



SEC Info

Source: <http://www.secinfo.com>

SEC Info offers the U.S. Securities and **Exchange Commission (SEC)** EDGAR database service on the web, with billions of links added to the SEC documents. It allows you to search by Name, Industry, and Business, SIC Code, Area Code, Accession Number, File Number, CIK, Topic, ZIP Code, etc.



The Search Monitor

Source: <http://www.thesearchmonitor.com>

The Search Monitor provides real-time competitive intelligence to monitor a number of things. It allows you to monitor market share, page rank, ad copy, landing pages, and the budget of your competitors. With the **trademark monitor**, you can monitor the buzz about yours as well as your competitor's brand and with the affiliate monitor; you can watch monitor ad and landing page copy.



Competitive Intelligence - What Expert Opinions Say About the Company



Copernic Tracker

Source: <http://www.copernic.com>

Copernic is website tracking software. It monitors a competitor's website continuously and acknowledges you content changes via an email, if any. The updated pages as well as the changes made in the site are highlighted for your convenience. You can even watch for specific keywords, to see the changes made on your **competitor's sites**.



SEMRush

Source: <http://www.semrush.com>

SEMRush is a competitive keyword research tool. For any site, you can get a list of Google keywords and AdWords, as well as a competitors list in the organic and paid Google search results. Necessary means for gaining in-depth knowledge about what competitors are advertising and their budget allocation to specific Internet marketing tactics are provided by SEMRush

Jobitorial



Source: <http://www.jobitorial.com>

Jobitorial provides anonymous employee reviews posted for jobs at thousands of companies and allows you to review a company.



AttentionMeter

Source: <http://www.attentionmeter.com>

AttentionMeter is a tool used for comparing any website you want (traffic) by using Alexa, Compete, and Quancast. It gives you a snapshot of traffic data as well as graphs from Alexa, Compete, and QuantCast.



ABI/INFORM Global

Source: <http://www.proquest.com>

ABI/INFORM Global is a business database. ABI/INFORM Global offers the latest business and financial information for researchers at all levels. With ABI/INFORM Global, users can determine business conditions, management techniques, business trends, management practice and theory, corporate strategy and tactics, and the competitive landscape.



Compete PRO

Source: <http://www.compete.com>

Compete PRO provides an online **competitive intelligence service**. It combines all the site, search, and referral analytics in a single product.



Footprinting Methodology



Footprinting using Google

Though Google is a search engine, the process of footprinting using Google is not similar to the process of footprinting through search engines. Footprinting using Google deals with gathering information by Google hacking. Google hacking is a hacking technique to **locate specific strings** of text within search results using an advanced operator in Google search engine. Google will filter for excessive use of advanced search operators and will drop the requests with the help of an Intrusion Prevention System



Footprinting using Google Hacking Techniques

Google hacking refers to the art of creating complex search engine queries. If you can construct proper queries, you can retrieve valuable data about a target company from the Google search results. Through Google hacking, an attacker tries to find websites that are vulnerable to numerous exploits and vulnerabilities. This can be accomplished with the help of Google hacking database (GHDB), a database of queries to identify sensitive data. Google operators help in finding required text and avoiding irrelevant data. Using advanced Google operators, attackers locate specific strings of text such as specific versions of vulnerable web applications.

Some of the popular Google operators include:

- ➊ **.Site:** The .Site operator in Google helps to find only pages that belong to a specific URL.
- ➋ **allinurl:** This operator finds the required pages or websites by restricting the results containing all query terms.
- ➌ **Inurl:** This will restrict the results to only websites or pages that contain the query terms that you have specified in the URL of the website.
- ➍ **allintitle:** It restricts results to only web pages that contain all the query terms that you have specified.

- ➊ **intitle:** It restricts results to only the web pages that contain the query term that you have specified. It will show only websites that mention the query term that you have used.
- ➋ **Inanchor:** It restricts results to pages containing the query term that you have specified in the anchor text on links to the page.
- ➌ **Allinanchor:** It restricts results to pages containing all query terms you specify in the anchor text on links to the page.



What Can a Hacker Do with Google Hacking?

If the target website is vulnerable to Google hacking, then the attacker can find the following with the help of queries in Google hacking database:

- ⌚ Error messages that contain sensitive information
- ⌚ Files containing passwords
- ⌚ Sensitive directories
- ⌚ Pages containing logon portals
- ⌚ Pages containing network or vulnerability data
- ⌚ Advisories and server vulnerabilities

Google Advance Search Operators

CEH
Certified Ethical Hacker

Google supports several advanced operators that help in modifying the search

[cache:]	 Displays the web pages stored in the Google cache
[link:]	 Lists web pages that have links to the specified web page
[related:]	 Lists web pages that are similar to a specified web page
[info:]	 Presents some information that Google has about a particular web page
[site:]	 Restricts the results to those websites in the given domain
[allintitle:]	 Restricts the results to those websites with all of the search keywords in the title
[intitle:]	 Restricts the results to documents containing the search keyword in the title
[allinurl:]	 Restricts the results to those with all of the search keywords in the URL
[inurl:]	 Restricts the results to documents containing the search keyword in the URL

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



Google Advance Search Operators

Source: <http://www.googleguide.com>

Cache: The CACHE query displays Google's cached version of a web page, instead of the current version of the page.

Example:

cache: www.eff.org will show Google's cached version of the Electronic Frontier Foundation home page.

Note: Do not put a space between cache: and the URL (web address).

link: Link lists web pages that have links to the specified web page. For example, to find pages that point to Google Guide's home page, enter:

link: www.googleguide.com

Note: According to Google's documentation, "you cannot combine a link: search with a regular keyword search."

Also note that when you combine link: with another advanced operator, Google may not return all the pages that match. The following queries should return lots of results, as you can see if you remove the -site: term in each of these queries.

related: If you start your query with "related:", then Google displays websites similar to the site mentioned in the search query.

Example: related:www.microsoft.com will provide the Google search engine results page with websites similar to microsoft.com.

info: Info will present some information the corresponding web page.

For instance, info:gothotel.com will show information about the national hotel directory GotHotel.com home page.

Note: There must be no space between the info: and the web page URL.

This functionality can also be obtained by typing the web page URL directly into a Google search box.

site: If you include site: in your query, Google will restrict your search results to the site or domain you specify.

For example, admissions site:www.lse.ac.uk will show admissions information from London School of Economics' site and [peace site:.gov] will find pages about peace within the .gov domain. You can specify a domain with or without a period, e.g., either as .gov or gov.

Note: Do not include a space between the "site:" and the domain.

allintitle: If you start your query with allintitle:, Google restricts results to those containing all the query terms you specify in the title.

For example, allintitle: detect plagiarism will return only documents that contain the words "detect" and "plagiarism" in the title. This functionality can also be obtained through the Advanced Web Search page, under Occurrences.

intitle: The query intitle: term restricts results to documents containing term in the title. For instance, flu shot intitle:help will return documents that mention the word "help" in their titles, and mention the words "flu" and "shot" anywhere in the document (title or not).

Note: There must be no space between the intitle: and the following word.

allinurl: If you start your query with allinurl:, Google restricts results to those containing all the query terms you specify in the URL.

For example, allinurl: google faq will return only documents that contain the words "google" and "faq" in the URL, such as "www.google.com/help/faq.html." This functionality can also be obtained through the Advanced Web Search page, under Occurrences.

In URLs, words are often run together. They need not be run together when you're using allinurl.

inurl: If you include inurl: in your query, Google will restrict the results to documents containing that word in the URL.

For instance, inurl:print site:www.googleguide.com searches for pages on Google Guide in which the URL contains the word "print." It finds PDF files that are in the directory or folder named "print" on the Google Guide website. The query [inurl:healthy eating] will return

documents that mention the words “healthy” in their URL, and mention the word “eating” anywhere in the document.

Note: There must be no space between the inurl: and the following word.

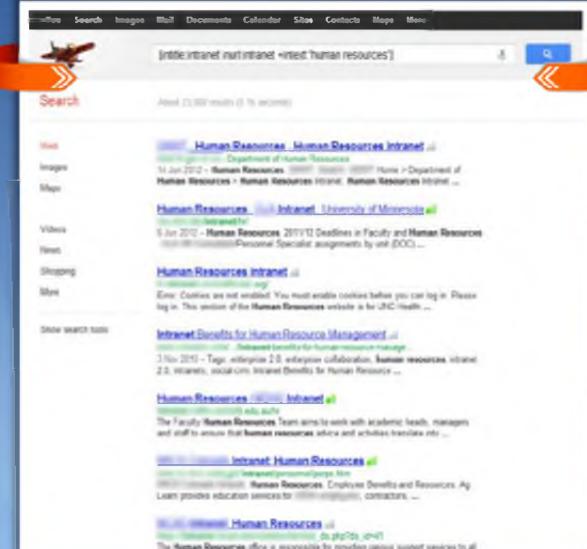
Finding Resources Using Google Advance Operator

[intitle:intranet inurl:intranet +intext:"human resources"]:

The above combination of the Google advanced search operators allows you to access a target company's private network and collect **sensitive information** such as **employee listings, key contact details**, etc. that can be incredibly useful for any social engineering endeavor



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



Finding Resources using Google Advance Operator

By using the Google Advance Operator syntax [intitle:intranet inurl:intranet +intext:"human resources"] : the attacker can find private information of a target company as well as sensitive information about the employees of that particular company. The information gathered by the attackers can be used to perform social engineering attacks. Google will filter for excessive use of advanced search operators and will drop the requests with the help of an Intrusion Prevention System.

The following screenshot shows a Google search engine results page displaying the results of the previously mentioned query:

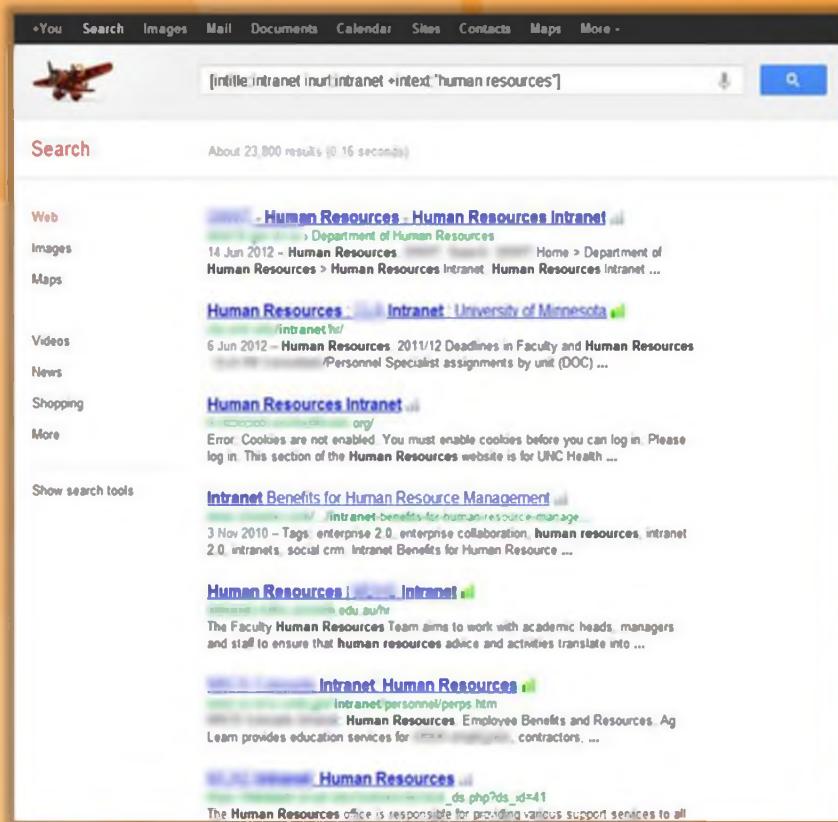


FIGURE 2.28: Search engine showing results for given Google Advance Operator syntax

Google Hacking Tool: Google Hacking Database (GHDB)

Advisories and Vulnerabilities

<http://www.hackersforcharity.org>

Pages Containing Login Portals

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



Google Hacking Tool: Google Hacking Database (GHDB)

Source: <http://www.hackersforcharity.org>

The Google Hacking database (GHDB) is a database of queries that identify sensitive data. GHDB is an **HTML/JavaScript wrapper application** that uses advanced JavaScript techniques to scrape information from Johnny's Google Hacking Database without the need for hosted server-side scripts. The Google Hacking Database exposes known issues with software that run websites. There are some bugs that expose information that might not warrant public reading.



FIGURE 2.29: Screenshots showing Advisories and Vulnerabilities & pages containing login portals

Google Hacking Tools

C|EH
Certified Ethical Hacker

 MetaGoofil http://www.edge-security.com	 Google Hack Honeypot http://ghh.sourceforge.net
 Goolink Scanner http://www.ghacks.net	 GMapCatcher http://code.google.com
 SiteDigger http://www.mcafee.com	 SearchDiggity http://www.stachilu.com
 Google Hacks http://code.google.com	 Google HACK DB http://www.secpoint.com
 BiLE Suite http://www.sensepost.com	 Gooscan http://www.darknet.org.uk

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



Google Hacking Tools

Besides the **Google Hacking Database** (GHDB) tool featured previously, there are some other tools that can help you with Google hacking. There are a few more Google hacking tools mentioned as follows. Using these tools, attackers can gather advisories and server vulnerabilities, error message information that may reveal attack paths, sensitive files, directories, logon portals, etc.



Metagoofil

Source: <http://www.edge-security.com>

Metagoofil is an **information-gathering tool** designed for extracting metadata of public documents (pdf, doc, xls, ppt, docx, ppts, xlsx) belonging to a target company.

Metagoofil performs a search in Google to identify and download the documents to a local disk and then extracts the metadata with different libraries such as Hachoir, PdfMiner?, and others. With the results, it generates a report with usernames, software versions, and servers or machine names that may help **penetration testers** in the information gathering phase.



Goolink Scanner

Source: <http://www.ghacks.net>

The Goolink Scanner **removes the cache** from your searches, and collects and displays only vulnerable site's links. Thus, it allows you to find vulnerable sites wide open to Google and googlebots.



SiteDigger

Source: <http://www.mcafee.com>

SiteDigger searches Google's cache to look for vulnerabilities, errors, configuration issues, proprietary information, and **interesting security nuggets** on websites.



Google Hacks

Source: <http://code.google.com>

Google Hacks is a compilation of carefully crafted Google searches that **expose novel functionality** from Google's search and map services. It allows you to view a timeline of your search results, view a map, search for music, search for books, and perform many other specific kinds of searches.



BiLE Suite

Source: <http://www.sensepost.com>

BiLE stands for **Bi-directional** Link Extractor. The BiLE suite includes a couple of Perl scripts used in enumeration processes. Each Perl script has its own functionality. BiLE.pl is the first tool or Perl script in the collection. BiLE leans on Google and HTTrack to automate the collections to and from the target site, and then applies a simple **statistical weighing algorithm** to deduce which websites have the strongest relationships with the target site.



Google Hack Honeypot

Source: <http://ghh.sourceforge.net>

Google Hack Honeypot is the reaction to a new type of **malicious web traffic**: search engine hackers. It is designed to provide reconnaissance against attackers that use search engines as a hacking tool against your resources. GHH implements the honeypot theory to provide additional security to your web presence.



GMapCatcher

Source: <http://code.google.com>

GMapCatcher is an **offline maps viewer**. It displays maps from many providers such as: CloudMade, OpenStreetMap, Yahoo Maps, Bing Maps, Nokia Maps, and SkyVector. maps.py is a GUI program used to browse Google map. With the offline toggle button unchecked, it can download Google map tiles automatically. Once the file downloads, it resides on your hard disk. Thus, you don't need to download it again.



SearchDiggity

Source: <http://www.stachliu.com>

SearchDiggity is the primary attack tool of the **Google Hacking Diggity Project**. It is Stach & Liu's MS Windows GUI application that serves as a front-end to the most recent versions of Diggity tools such as GoogleDiggity, BingDiggity, Bing LinkFromDomainDiggity, CodeSearchDiggity, DLPDiggity, MalwareDiggity, PortScanDiggity, SHODANDiggity, BingBinaryMalwareSearch, and NotInMyBackYard Diggity.



Google HACK DB

Source: <http://www.secpoint.com>

The attacker can also use the SecPoint Google HACK DB tool to determine sensitive information from the target site. This tool helps an attacker to extract files containing passwords, database files, clear text files, customer database files, etc.



Gooscan

Source: <http://www.darknet.org.uk>

Gooscan is a tool that automates queries against **Google search appliances**. These queries are designed to find potential vulnerabilities on web pages.



Footprinting Methodology

Gathering **network-related** information such as whois information of the target organization is very important when hacking a system. So, now we will discuss whois footprinting.

Whois footprinting focuses on how to perform a whois lookup, analyzing the whois lookup results, and the tools to gather whois information.

WHOIS Lookup

WHOIS databases are maintained by **Regional Internet Registries** and contain the **personal information of domain owners**

WHOIS query returns:

- Domain name details
- Contact details of domain owner
- Domain name servers
- NetRange
- When a domain has been created
- Expiry records
- Records last updated

Information obtained from WHOIS database assists an attacker to:

- Create detailed map of organizational network
- Gather personal information that assists to perform social engineering
- Gather other internal network details, etc.

Regional Internet Registries (RIRs)

AFRINIC ARIN APNIC RIPE NCC LACNIC

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



WHOIS Lookup

WHOIS is a query and response protocol used for **querying databases** that stores the registered users or assignees of an Internet resource, such as a domain name, an IP address block, or an autonomous system. WHOIS databases are maintained by Regional Internet Registries and contain the personal information of domain owners. They maintain a record called a **LOOKUP table** that contains all the information associated with a particular network, domain, and host. Anyone can connect and query to this server to get information about particular networks, domains, and hosts.

An attacker can send a query to the appropriate **WHOIS** server to obtain the information about the target domain name, contact details of its owner, expiry date, creation date, etc. The WHOIS sever will respond to the query with respective information. Then, the attacker can use this information to create a map of the organization network, trick domain owners with social engineering once he or she gets contact details, and then get **internal details** of the network.

The screenshot displays two side-by-side web pages for domain analysis.

Left Panel (Whois.domaintools.com):

- Registrant:** Domain Administrator, Microsoft Corporation, One Microsoft Way, Redmond WA 98052, US. Email: domains@microsoft.com, Phone: +1.4259367329.
- Domain Name:** microsoft.com
- Registrar Name:** Markmonitor.com
- Administrative Contact:** Domain Administrator, Microsoft Corporation, One Microsoft Way, Redmond WA 98052, US. Email: domains@microsoft.com, Phone: +1.4259367329.
- Technical Contact:** NSM Hostmaster, Microsoft Corporation, One Microsoft Way, Redmond WA 98052, US. Email: msnhost@microsoft.com, Phone: +1.4268828080, Fax: +1.4269367329.
- Created on:** 1991-05-01. **Expires on:** 2021-05-02. **Record last updated on:** 2011-08-14.
- Domain servers in listed order:** cs0.mact.net, cs4.mact.net, cs1.mact.net, cs3.mact.net, ms2.mact.net.

<http://whois.domaintools.com>

Right Panel (Domain Dossier):

- Domain Dossier** logo: A person icon.
- Domain or IP address:** juggyboy.com
- Options:** domain whois record (checked), DNS records, network whois record (checked), traceroute, service scan.
- Address lookup:** canonical name: juggyboy.com, aliases, addresses.
- Domain Whois record:** Domain Name: JUGGYBOY.COM, Registrant: NETWORK SOLUTIONS, INC., Name Server: NS01.NETWORKSOLUTIONS.COM, Referral URL: http://www.networksolutions.com/en_US/, Name Server: NS02.WORLDNIC.COM, Status: clientTransferProhibited, Updated Date: 03-feb-2009, Creation Date: 16-jul-2002, Expiration Date: 14-jul-2014.
- Log:** >>> Last update of whois database: Thu, 19 Jul 2012 07:49:34 UTC <<<
- Queried:** whois.networksolutions.com with juggyboy.com...
- Registrant:** NETWORKSOLUTIONS.COM, Inc., 2000 University Street, Seattle, WA 98101, USA, 206-467-XXXX.

<http://centralops.net/co>

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



WHOIS Lookup Result Analysis

A whois lookup can be performed using Whois services such as <http://whois.domaintools.com> or <http://centralops.net/co>. Here you can see the result analysis of a Whois lookup obtained with the two mentioned Whois services. Both these services allow you to perform a whois lookup by entering the target's domain or IP address. The domaintools.com service provides whois information such as registrant information, email, administrative contact information, created and expiry date, a list of domain servers, etc. The Domain Dossier available at <http://centralops.net/co/> gives the address lookup, domain Whois record, network whois record, and **DNS records information**.

Whois Record

Registrant:
Domain Administrator
Microsoft Corporation
One Microsoft Way
Redmond WA 98052
US
domains@microsoft.com +1.4258828080 Fax: +1.4259367329

Domain Name: microsoft.com

Registrar Name: Markmonitor.com
Registrar Whois: whois.markmonitor.com
Registrar Homepage: http://www.markmonitor.com

Administrative Contact:
Domain Administrator
Microsoft Corporation
One Microsoft Way
Redmond WA 98052
US
domains@microsoft.com +1.4258828080 Fax: +1.4259367329

Technical Contact, Zone Contact:
MSN Hostmaster
Microsoft Corporation
One Microsoft Way
Redmond WA 98052
US
msnhst@microsoft.com +1.4258828080 Fax: +1.4259367329

Created on.....: 1991-05-01.
Expires on.....: 2021-05-02.
Record last updated on..: 2011-08-14.

Domain servers in listed order:
ns5.msft.net
ns4.msft.net
ns1.msft.net
ns3.msft.net
ns2.msft.net

Domain Dossier Investigate domains and IP addresses

domain or IP address: **juggyboy.com**

domain whois record DNS records traceroute
 network whois record service scan

user: anonymous [30]
balance: 47 units
[log in](#) | [account info](#)

Address lookup
canonical name: **juggyboy.com**.
aliases
addresses: [REDACTED] 6

Domain Whois record
Queried whois.internic.net with "dom juggyboy.com"...

Domain Name: JUGGYBOY.COM
Registrar: NETWORK SOLUTIONS, LLC.
Whois Server: whois.networksolutions.com
Referral URL: http://www.networksolutions.com/en_US/
Name Server: NS10.WORLDCOM.COM
Name Server: NS20.WORLDCOM.COM
Status: clientTransferProhibited
Updated Date: 03-feb-2009
Creation Date: 16-jul-2002
Expiration Date: 16-jul-2014

>>> Last update of whois database: Thu, 19 Jul 2012 07:49:36 UTC <<<
Queried whois.networksolutions.com with "juggyboy.com"...

Registrant:
[REDACTED]
Jesse Johnson
c/o DCI Network Solutions
PO Box 410
Durham, NC 27702

<http://whois.domaintools.com>

<http://centralops.net/co>

FIGURE 2.30: Whois services screenshots

The image shows a screenshot of the SmartWhois software interface. At the top, there's a banner with the text "WHOIS Lookup Tool: SmartWhois" and the CEH logo. Below the banner, there's a cartoon illustration of a person sitting at a desk with a computer monitor. To the right of the illustration is a window titled "SmartWhois - Evaluation Version". The window has a toolbar with various icons. In the main area, the search bar contains "microsoft.com". The results pane shows the following information for "microsoft.com":

- Free SAS / ProXad
- 8, rue de la ville l'Eveque
- 75008 Paris
- phone +33 1 73 50 20 00
- fax +33 1 73 50 25 01
- hostmaster@proxad.net
- Free SAS / ProXad
- 8, rue de la ville l'Eveque
- 75008 Paris
- phone +33 1 73 50 20 00
- fax +33 1 73 50 25 01
- hostmaster@proxad.net
- frams1-q20@frams.fr [212.27.60.19]
- frams2-q20@frams.fr [212.27.60.20]
- Google Page Rank: 7
- Axes Traffic Rank: 11,130
- Created: 20/12/2008
- Updated: 17/02/2004
- Source: whois.mcr

At the bottom of the window, it says "Completed at: 19-07-2012 12:48:01 PM" and "Processing time: 1.65 seconds". There's also a link "View SOURCE".

<http://www.tamos.com>

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



WHOIS Lookup Tool: SmartWhois

Source: <http://www.tamos.com>

SmartWhois is a useful **network information** utility that allows you to look up all the available information about an IP address, hostname, or domain, including country, state or province, city, name of the network provider, administrator, and technical support contact information. It also assists you in finding the owner of the domain, the owner's contact information, the owner of the **IP address block**, registered date of the domain, etc.

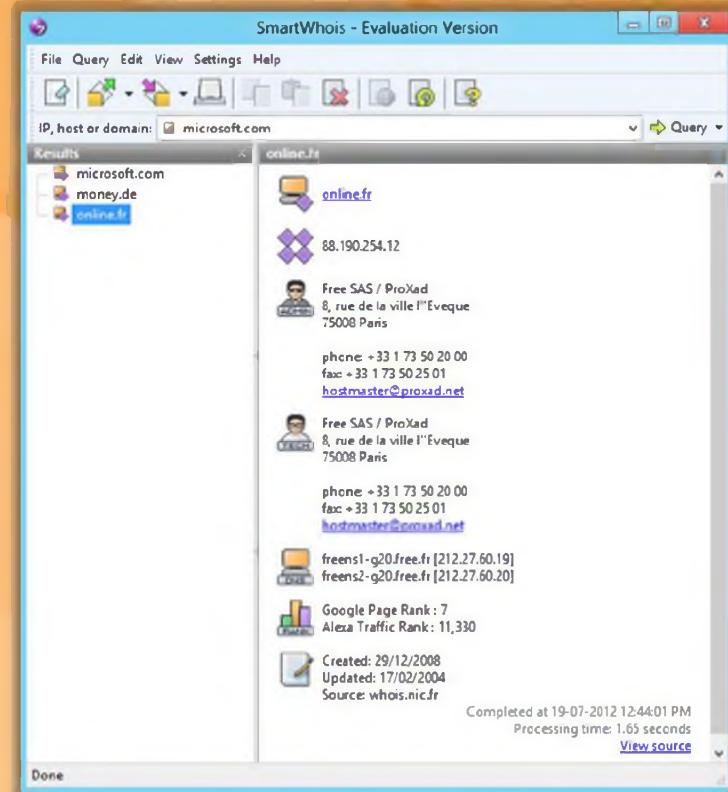


FIGURE 2.31: SmartWhois screenshot

WHOIS Lookup Online Tools

C|EH
Certified Ethical Hacker

 SmartWhois http://smartwhois.com	 Whois http://tools.whois.net
 Better Whois http://www.betterwhois.com	 DNSstuff http://www.dnsstuff.com
 Whois Source http://www.whois.sc	 Network Solutions Whois http://www.networksolutions.com
 Web Wiz http://www.webwiz.co.uk/domain-tools/whois-lookup.htm	 WebToolHub http://www.webtoothub.com/tn561381-whois-lookup.aspx
 Network-Tools.com http://network-tools.com	 Ultra Tools https://www.ultratools.com/whois/home

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



WHOIS Lookup Tools

Similar to SmartWhois, there are numerous tools available in the market to retrieve Whois information. A few are mentioned as follows:



CountryWhois

Source: <http://www.tamos.com>

CountryWhois is a utility for identifying the **geographic location of an IP address**. CountryWhois can be used to analyze server logs, check email address headers, identify online credit card fraud, or in any other instance where you need to quickly and accurately determine the country of origin by IP address.



LanWhoIs

Source: <http://lantricks.com>

LanWhoIs provides information about **domains** and **addresses** on the Internet. This program helps you determine who, where, and when the domain or site you are interested in was registered, and the information about those who support it now. This tool allows you to save your search result in the form of an archive to view it later. You can print and save the search result in HTML format.



Batch IP Converter

Source: <http://www.networkmost.com>

Batch IP Converter is a network tool to work with IP addresses. It combines Domain-to-IP Converter, Batch Ping, Tracert, Whois, Website Scanner, and Connection Monitor into a single interface as well as an **IP-to-Country Converter**. It allows you to look up the IP address for a single or list of domain names and vice versa.



CallerIP

Source: <http://www.calleripro.com>

CallerIP is basically IP and port monitoring software that displays the incoming and outgoing connection made to your computer. It also allows you to find the origin of all connecting IP addresses on the world map. The Whois reporting feature provides key information such as who an IP is registered to along with **contact email addresses** and **phone numbers**.



WhoIs Lookup Multiple Addresses

Source: <http://www.sobolsoft.com>

This software offers a solution for users who want to **look up ownership details** for one or more IP addresses. Users can simply enter **IP addresses** or load them from a file. There are three options for lookup sites: whois.domaintools.com, whois-search.com, and whois.arin.net. The user can set a delay period between lookups, to avoid lockouts from these websites. The resulting list shows the IP addresses and details of each. It also allows you to save results to a text file.



WhoIs Analyzer Pro

Source: <http://www.whoisanalyzer.com>

This tool allows you to access information about a **registered domain worldwide**; you can view the domain owner name, domain name, and contact details of domain owner. It also helps in finding the location of a specific domain. You can also submit multiple queries with this tool simultaneously. This tool gives you the ability to print or save the result of the query in **HTML format**.



HotWhois

Source: <http://www.tialsoft.com>

HotWhois is an IP tracking tool that can **reveal valuable information**, such as country, state, city, address, contact phone numbers, and email addresses of an IP provider. The query mechanism resorts to a variety of Regional Internet Registries, to obtain IP Whois information about IP address. With HotWhois you can make whois queries even if the registrar, supporting a particular domain, doesn't have the **whois server itself**.



Whois 2010 Pro

Source: <http://lapshins.com>

Whois 2010 PRO is **network information software** that allows you to look up all the available information about a domain name, including country, state or province, city, administrator, and technical support contact information.



ActiveWhois

Source: <http://www.johnru.com>

ActiveWhois is a network tool to find information about the owners of IP addresses or Internet domains. You can determine the country, personal and postal addresses of the owner, and/or users of IP addresses and domains.



WhoisThisDomain

Source: <http://www.nirsoft.net>

WhoisThisDomain is a domain registration lookup utility that allows you to get information about a registered domain. It automatically connects to the right WHOIS server and retrieves the WHOIS record of the domain. It supports both generic domains and country code domains.

WHOIS Lookup Online Tools

C|EH
Certified Ethical Hacker

 SmartWhois http://smartwhois.com	 Whois http://tools.whois.net
 Better Whois http://www.betterwhois.com	 DNSstuff http://www.dnsstuff.com
 Whois Source http://www.whois.sc	 Network Solutions Whois http://www.networksolutions.com
 Web Wiz http://www.webwiz.co.uk/domain-tools/whois-lookup.htm	 WebToolHub http://www.webtoolhub.com/tn561381-whois-lookup.aspx
 Network-Tools.com http://network-tools.com	 Ultra Tools https://www.ultratools.com/whois/home

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



WHOIS Lookup Online Tools

In addition to the Whois lookup tools mentioned so far, a few online Whois lookup tools are listed as follows:

- ⌚ SmartWhois available at <http://smartwhois.com>
- ⌚ Better Whois available at <http://www.betterwhois.com>
- ⌚ Whois Source available at <http://www.whois.sc>
- ⌚ Web Wiz available at <http://www.webwiz.co.uk/domain-tools/whois-lookup.htm>
- ⌚ Network-Tools.com available at <http://network-tools.com>
- ⌚ Whois available at <http://tools.whois.net>
- ⌚ DNSstuff available at <http://www.dnsstuff.com>
- ⌚ Network Solutions Whois available at <http://www.networksolutions.com>
- ⌚ WebToolHub available at <http://www.webtoolhub.com/tn561381-whois-lookup.aspx>
- ⌚ Ultra Tools available at <https://www.ultratools.com/whois/home>



Footprinting Methodology

The next phase in footprinting methodology is DNS footprinting.

This section describes how to extract DNS information and the **DNS interrogation** tools.

Extracting DNS Information

C|EH
Certified Ethical Hacker

Attacker can gather DNS information to determine key hosts in the network and can perform social engineering attacks

DNS records provide important information about location and type of servers

Record Type	Description
A	Points to a host's IP address
MX	Points to domain's mail server
NS	Points to host's name server
CNAME	Canonical naming allows aliases to a host
SOA	Indicate authority for domain
SRV	Service records
PTR	Maps IP address to a hostname
RP	Responsible person
HINFO	Host Information record includes CPU type and OS
TXT	Unstructured text records

DNS Interrogation Tools

- http://www.dnsstuff.com
- http://network-tools.com

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



Extracting DNS Information

DNS footprinting allows you to obtain information about **DNS zone data**. This DNS zone data includes DNS domain names, computer names, IP addresses, and much more about a particular network. The attacker performs **DNS footprinting** on the target network in order to obtain the information about DNS. He or she then uses the gathered DNS information to determine key hosts in the network and then performs social engineering attacks to gather more information.

DNS footprinting can be performed using DNS interrogation tools such as www.DNSstuff.com. By using www.DNSstuff.com, it is possible to extract DNS information about IP addresses, mail server extensions, DNS lookups, Whois lookups, etc. If you want information about a target company, it is possible to extract its range of IP addresses utilizing the **IP routing** lookup of DNS stuff. If the target network allows unknown, unauthorized users to transfer DNS zone data, then it is easy for you to obtain the information about DNS with the help of the DNS interrogation tool.

Once you send the query using the DNS interrogation tool to the **DNS server**, the server will respond to you with a record structure that contains information about the target DNS. DNS records provide important information about location and type of servers.

- A - Points to a host's IP address

- ⌚ MX - Points to domain's mail server
- ⌚ NS - Points to host's name server
- ⌚ CNAME - Canonical naming allows aliases to a host
- ⌚ SOA - Indicate authority for domain
- ⌚ SRV - Service records
- ⌚ PTR - Maps IP address to a hostname
- ⌚ RP - Responsible person
- ⌚ HINFO - Host information record includes CPU type and OS

A few more examples of DNS interrogation tools to send a DNS query include:

- ⌚ <http://www.dnsstuff.com>
- ⌚ <http://network-tools.com>

Extracting DNS Information (Cont'd)

This tool is very useful to perform a DNS query on any host. Each domain name (Example: dnsqueries.com) is structured in hosts (ex: dnsqueries.com) and the DNS (Domain Name System) allows anyone to translate the domain name or the hostname in an IP Address to contact via the TCP/IP protocol. There are several types of queries, corresponding to all the implementable types of DNS records such as A record, MX, AAAA, CNAME and SOA.

Perform DNS query

HostName: microsoft.com

Type: ANY

Run tool »

Results for checks on microsoft.com

Host	TTL	Class	Type	Details
microsoft.com	3381	IN	TXT	FbUF6DbkE+AwI/wi9xgD8KvrlZus5v8L6tbIQ2kGrQ/rVQKj8CjQbBTWtE64ey4NJw/j5J65PiggVYNabd==
microsoft.com	3381	IN	TXT	v=spf1 include:_spf-a.microsoft.com include:_spf-b.microsoft.com include:_spf-c.microsoft.com include:_spf-ssg-a.microsoft.com ip4:131.107.115.215 ip4:131.107.115.214 ip4:205.248.106.64 ip4:205.248.106.30 ip4:205.248.106.32 ~all
microsoft.com	3381	IN	MX	10 mail.messaging.microsoft.com
microsoft.com	3381	IN	SOA	ns1.msft.net msnhst.microsoft.com 2012071602 300 600 2419200 3000
microsoft.com	3381	IN	A	64.4.11.37
microsoft.com	3381	IN	A	65.55.58.201
microsoft.com	141531	IN	NS	ns5.msft.net
microsoft.com	141531	IN	NS	ns2.msft.net
microsoft.com	141531	IN	NS	ns1.msft.net
microsoft.com	141531	IN	NS	ns3.msft.net
microsoft.com	141531	IN	NS	ns4.msft.net

http://www.dnsqueries.com

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



Extracting DNS Information (Cont'd)

Source: <http://www.dnsqueries.com>

Perform DNS query available at <http://www.dnsqueries.com> is a tool that allows you to perform a DNS query on any host. Each domain name (example: dnsqueries.com) is structured in hosts (ex: www.dnsqueries.com) and the DNS (Domain Name System) allows anyone to translate the domain name or the hostname in an IP address to contact via the **TCP/IP protocol**. There are several types of queries, corresponding to all the implementable types of DNS records such as a record, MX, AAAA, CNAME, and SOA.

Now let's see how the DNS interrogation tool retrieves information about the DNS. Go to the browser and type <http://www.dnsqueries.com> and press Enter. The DNS query's homesite will be displayed in the browser.

Enter the domain name of your interest in the Perform **DNS query's HostName** field (here we are entering Microsoft.com) and click the Run tool button; the DNS information for Microsoft.com will be displayed as shown in the following figure.

This tool is very useful to perform a DNS query on any host. Each domain name (Example: dnsqueries.com) is structured in hosts (ex: www.dnsqueries.com) and the DNS (Domain Name System) allow everybody to translate the domain name or the hostname in an IP Address to contact via the TCP/IP protocol. There are several types of queries, corresponding to all the implementable types of DNS records such as A record, MX, AAAA, CNAME and SOA.

Perform DNS query

HostName:

Type:

Results for checks on microsoft.com

Host	TTL	Class	Type	Details
microsoft.com	3381	IN	TXT	FbUF6DbkE+Aw1/wi9xgDi8KvrIZus5v8L6tbIQZkGrQ/-VQKJiBCjQbBtWtE64ey4NJJwvj5J65PiggVNabdQ--
microsoft.com	3381	IN	TXT	v=spf1 include:_spf-a.microsoft.com include:_spf-b.microsoft.com include:_spf-c.microsoft.com include:_spf-ssgb.a.microsoft.com ip4:131.107.115.215 ip4:131.107.115.214 ip4:205.248.106.64 ip4:205.248.106.30 ip4:205.248.106.32 ~all
microsoft.com	3381	IN	A	10 mail.messaging.microsoft.com
microsoft.com	3381	IN	SOA	ns1.msft.net msnhst.microsoft.com 2012071602 300 600 2419200 3600
microsoft.com	3381	IN	A	64.4.11.37
microsoft.com	3381	IN	A	65.55.58.201
microsoft.com	141531	IN	NS	ns5.msft.net
microsoft.com	141531	IN	NS	ns2.msft.net
microsoft.com	141531	IN	NS	ns1.msft.net
microsoft.com	141531	IN	NS	ns3.msft.net
microsoft.com	141531	IN	NS	ns4.msft.net

FIGURE 2.32: Screenshot showing DNS information for Microsoft.com

DNS Interrogation Tools

C|EH
Certified Ethical Hacker

 DIG http://www.kloth.net	 DNSWatch http://www.dnswatch.info
 myDNSTools http://www.mydnstools.info	 DomainTools http://www.domaintools.com
 Professional Toolset http://www.dnsstuff.com	 DNS http://e-dns.org
 DNS Records http://network-tools.com	 DNS Lookup Tool http://www.webwiz.co.uk
 DNSData View http://www.nirsoft.net	 DNS Query Utility http://www.webmaster-toolkit.com

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



DNS Interrogation Tools

A few more well-known **DNS interrogation** tools are listed as follows:

- ⌚ DIG available at <http://www.kloth.net>
- ⌚ myDNSTools available at <http://www.mydnstools.info>
- ⌚ Professional Toolset available at <http://www.dnsstuff.com>
- ⌚ DNS Records available at <http://network-tools.com>
- ⌚ DNSData View available at <http://www.nirsoft.net>
- ⌚ DNSWatch available at <http://www.dnswatch.info>
- ⌚ DomainTools Pro available at <http://www.domaintools.com>
- ⌚ DNS available at <http://e-dns.org>
- ⌚ DNS Lookup Tool available at <http://www.webwiz.co.uk>
- ⌚ DNS Query Utility available at <http://www.webmaster-toolkit.com>



Footprinting Methodology

The next step after retrieving the DNS information is to gather **network-related** information. So, now we will discuss network footprinting, a method of gathering network-related information.

This section describes how to locate network range, determine the operating system, Traceroute, and the **Traceroute tools**.

Locate the Network Range

C|EH
Certified Ethical Hacker

- Network range information obtained assists an attacker to create a **map of the target's network**
- Find the **range of IP addresses** using **ARIN whois database search tool**
- You can find the range of IP addresses and the subnet mask used by the target organization from **Regional Internet Registry (RIR)**

Network Whois Record

```
Queried whois.arin.net with "n 207.46.232.182"...

NetRange: 207.46.0.0 - 207.46.255.255
CIDR: 207.46.0.0/16
OriginAS:
NetName: MICROSOFT-GLOBAL-NET
NetHandle: NET-207-46-0-0-1
Parent: NET-207-0-0-0-0
NetType: Direct Assignment
NameServer: NS2.MSFT.NET
NameServer: NS4.MSFT.NET
NameServer: NS1.MSFT.NET
NameServer: NS5.MSFT.NET
NameServer: NS3.MSFT.NET
RegDate: 1997-03-31
Updated: 2004-12-09
Ref: http://whois.arin.net/rest/net/NET-207-46-0-0-1
OrgName: Microsoft Corp
OrgId: MSFT
Address: One Microsoft Way
City: Redmond
StateProv: WA
PostalCode: 98052
Country: US
RegDate: 1998-07-10
Updated: 2009-11-10
Ref: http://whois.arin.net/rest/org/MSFT
OrgAbuseHandle: ABUSE231-ARIN
OrgAbuseName: Abuse
OrgAbusePhone: +1-425-882-8080
OrgAbuseEmail: abuse@hotmail.com
OrgAbuseRef: http://whois.arin.net/rest/poc/ABUSE231-ARIN
```

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



Locate the Network Range

To perform network footprinting, you need to **gather basic and important information** about the target organization such as what the organization does, who they work for, and what type of work they perform. The answers to these questions give you an idea about the internal structure of the target network.

After gathering the aforementioned information, an attacker can proceed to find the network range of a target system. He or she can get more detailed information from the appropriate regional registry database regarding IP allocation and the nature of the allocation. An attacker can also determine the subnet mask of the domain. He or she can also trace the route between the system and the target system. Two popular **traceroute tools** are NeoTrace and Visual Route.

Obtaining private IP addresses can be useful for an attacker. The Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of the IP address space for private Internets: 10.0.0.0–10.255.255.255 (10/8 prefix), 172.16.0.0–172.31.255.255 (172.16/12 prefix), and 192.168.0.0–192.168.255.255 (192.168/16 prefix).

The network range gives you an idea about how the network is, which machines in the networks are alive, and it helps to identify the network topology, access control device, and OS

used in the target network. To find the **network range** of the target network, enter the server IP address (that was gathered in **WHOIS footprinting**) in the ARIN whois database search tool or you can go to the ARIN website (<https://www.arin.net/knowledge/rirs.html>) and enter the server IP in the SEARCH Whois text box. You will get the network range of the target network. If the DNS servers are not set up correctly, the attacker has a good chance of obtaining a list of internal machines on the server. Also, sometimes if an attacker traces a route to a machine, he or she can get the internal IP address of the **gateway**, which might be useful.

Network Whois Record

```
Queried whois.arin.net with "n 207.46.232.182"...

NetRange:      207.46.0.0 - 207.46.255.255
CIDR:         207.46.0.0/16
OriginAS:
NetName:       MICROSOFT-GLOBAL-NET
NetHandle:     NET-207-46-0-0-1
Parent:        NET-207-0-0-0-0
NetType:       Direct Assignment
NameServer:   NS2.MSFT.NET
NameServer:   NS4.MSFT.NET
NameServer:   NS1.MSFT.NET
NameServer:   NS5.MSFT.NET
NameServer:   NS3.MSFT.NET
RegDate:      1997-03-31
Updated:       2004-12-09
Ref:          http://whois.arin.net/rest/net/NET-
207-46-0-0-1
OrgName:       Microsoft Corp
OrgId:         MSFT
Address:      One Microsoft Way
City:          Redmond
StateProv:    WA
PostalCode:   98052
Country:      US
RegDate:      1998-07-10
Updated:       2009-11-10
Ref:          http://whois.arin.net/rest/org/MSFT
OrgAbuseHandle: ABUSE231-ARIN
OrgAbuseName:  Abuse
OrgAbusePhone: +1-425-882-8080
OrgAbuseEmail: abuse@hotmail.com
OrgAbuseRef:
http://whois.arin.net/rest/poc/ABUSE231-ARIN
```

You need to use more than one tool to obtain network information as sometimes a single tool is not capable of delivering the information you want.

Determine the Operating System

Use the **Netcraft** tool to determine the OSes in use by the target organization

The screenshot shows the Netcraft homepage with a search bar for 'microsoft'. Below the search bar, there's a table titled 'Results for microsoft' listing 252 sites. Each row contains the site URL, first seen date, last check date, and the operating system (OS) running on that site. The OS column includes entries like 'windows xp', 'windows server 2008', 'windows 7', 'windows 8', etc. To the right of the main search results, there's a separate table titled 'Sites with IIS6 running instances at Microsoft.com' showing various Microsoft websites and their IIS versions.



Determine the Operating System

Source: <http://news.netcraft.com>

So far we have collected information about IP addresses, network ranges, server names, etc. of the target network. Now it's time to find out the **OS running** on the **target network**. The technique of obtaining information about the target network OS is called **OS fingerprinting**. The Netcraft tool will help you to find out the OS running on the target network.

Let's see how Netcraft helps you determine the OS of the target network.

Open the <http://news.netcraft.com> site in your browser and type the domain name of your target network in the What's that site running? field (here we are considering the domain name "Microsoft.com"). It displays all the **sites associated** with that domain along with the operating system running on each site.

Site	Site Report	First seen	Netblock	OS
1. www.microsoft.com		august 1995	microsoft corp	cbrix netscaler
2. support.microsoft.com		october 1997	microsoft corp	unknown
3. isophilic.microsoft.com		august 1999	microsoft corp	cbrix netscaler
4. windows.microsoft.com		june 1998	microsoft corp	windowse server 2008
5. mads.microsoft.com		september 1998	microsoft corp	cbrix netscaler
6. @fca.microsoft.com		november 1998	microsoft corp	unknown
7. social.technet.microsoft.com		august 2008	microsoft corp	cbrix netscaler
8. answers.microsoft.com		august 2009	microsoft limited	windowse server 2008
9. www.update.microsoft.com		may 2007	microsoft corp	windowse server 2008
10. social.msn.microsoft.com		august 2008	microsoft corp	cbrix netscaler
11. ge.microsoft.com		november 2001	ms hotmail	cbrix netscaler
12. windowsupdate.microsoft.com		february 1999	microsoft corp	windowse server 2008
13. update.microsoft.com		february 2005	microsoft corp	windowse server 2008
14. www.microsofttranslator.com		november 2008	akamai technologies	linux
15. search.microsoft.com		january 1997	akamai international b.v	linux
16. www.microsoftstore.com		november 2008	digital river ireland ltd.	f5 big-ip
17. login.microsoftonline.com		december 2010	microsoft corp	windowse server 2008
18. ver.microsoft.com		october 2003	microsoft corp	windowse server 2008

OS, Web Server and Hosting History for windows.microsoft.com				
http://Windows.microsoft.com was running Microsoft IIS 6.0 F5 BIG-IP when last queried at 1-Aug-2012 19:31:10 CDT - refresh now Site Report				
Get the Netcraft Toolbar!				
OS	Server	Last changed	IP address	Netblock Owner
F5 BIG-IP	Microsoft-4S/7.5	18-Jun-2012	65.55.175.183	Microsoft Corp
F5 BIG-IP	Microsoft-4S/7.5	14-Jun-2012	65.55.175.183	Microsoft Corp
F5 BIG-IP	Microsoft-4S/7.5	18-Jun-2012	66.66.81.30	Microsoft Corp
F5 BIG-IP	Microsoft-4S/7.5	14-Jun-2012	65.55.175.183	Microsoft Corp
F5 BIG-IP	Microsoft-4S/7.5	10-Mar-2012	65.55.175.183	Microsoft Corp
F5 BIG-IP	Microsoft-4S/7.5	14-May-2012	66.66.175.183	Microsoft Corp
F5 BIG-IP	Microsoft-4S/7.5	10-Apr-2012	66.62.103.234	Microsoft Corp
F5 BIG-IP	Microsoft-4S/7.5	12-Apr-2012	65.52.103.234	Microsoft Corp
F5 BIG-IP	Microsoft-4S/7.5	16-Mar-2012	65.52.103.234	Microsoft Corp
F5 BIG-IP	Microsoft-4S/7.5	11-Mar-2012	66.66.175.183	Microsoft Corp

Sites with keepalive running systems at Microsoft Corp						
Microsoft Corp does Microsoft Way (Received via US 99652)						
Note: Uptime : the time since last reboot is explained in the FAQ						
Rank	Site	Average	Max	Latent		
OS	Server					
1	www.pasaport.com	60	129	3	Windows Server 2008	Microsoft-4S/7.5
2	www.encastra.com	52	98	2	F5 BIG-IP	DigiF
3	astiblitz.com	48	91	76	Windows Server 2008	Microsoft-4S/7.0
4	www.capitol.com	46	81	81	unknown	Microsoft-4S/7.5
5	modie.com	41	55	55	unknown	Microsoft-4S/7.5
6	msresol.com.br	39	39	49	unknown	Microsoft-4S/7.5
7	msresol.ru	38	50	61	unknown	Microsoft-4S/7.5
8	msgrabsalone.microsoft.com	38	84	25	unknown	Microsoft-4S/7.5
9	cgi.microsoft.com	36	66	66	F5 BIG-IP	Microsoft-4S/7.5
10	www.12121.net	33	77	72	Windows Server 2008	Microsoft-HIT-IPNP12.0
11	msresol.com	32	45	27	unknown	Microsoft-4S/7.5
12	www.man.com.tw	30	82	38	F5 BIG-IP	Microsoft-4S/7.5
13	cab.com	29	50	4	F5 BIG-IP	Microsoft-4S/7.5
14	www.OFFICE.COM	20	185	115	F5 BIG-IP	Microsoft-4S/7.5
15	office.microsoft.com	25	110	10	F5 BIG-IP	Microsoft-4S/7.5
16	blgo.bethelnet.com	26	20	28	Windows Server 2003	Microsoft-4S/7.5
17	www.microsoft.com	24	45	9	unknown	Microsoft-4S/7.5
18	10.man.com	22	24	25	Calm Networks	Microsoft-4S/7.5
19	man.or.jp	22	36	28	F5 BIG-IP	Microsoft-4S/7.5
20	LIVE.COM	20	51	18	unknown	Microsoft-4S/7.5
21	man.org	18	75	4	unknown	Microsoft-4S/7.5

FIGURE 2.33: Netcraft showing the operating system that is in use by Microsoft

The screenshot shows the SHODAN search interface. On the left, there's a sidebar with icons for cameras, routers, servers, and switches. Below it, a section titled "EXPOSE ONLINE DEVICES." features a world map where many countries are highlighted in red, indicating found devices. Text on the sidebar says: "Use SHODAN search engine that lets you find specific computers (routers, servers, etc.) using a variety of filters". The main search results page has a header "SHODAN" and a search bar. It displays a table of results for "Microsoft" with columns for "Services", "Top Countries", and "Results". The first result is for "Microsoft IIS". The right side of the screen shows detailed logs for three different Microsoft IIS entries, including headers like "HTTP/1.1 200 OK", "Content-Type: text/html", and "Server: Microsoft-IIS/6.0". At the bottom, a copyright notice reads: "Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited."

Determine the Operating System (Cont'd)



SHODAN Search Engine

Source: <http://www.shodanhq.com>

Use SHODAN search engine that lets you find specific computers (routers, servers, etc.) using a variety of filters.

The screenshot shows the SHODAN homepage. The top features a search bar and a large banner with the text "EXPOSE ONLINE DEVICES." and a world map. Below the banner are two buttons: "TAKE A TOUR" and "FREE SIGN UP". At the bottom, there are three sections: "DEVELOPER API", "LEARN MORE", and "FOLLOW ME". The "DEVELOPER API" section includes a Python code snippet for interacting with the Shodan database. The "LEARN MORE" section provides links to documentation and forums. The "FOLLOW ME" section features a blue bird icon and a link to the Shodan blog. Popular search queries are listed at the bottom: "RuggedCom exposed via Telnet", "Wired: http://www.wired.com/threatlevel/2012/04/ruggedcom-backdoor", and "Full Disclosure: http://sec...".

FIGURE 2.34: SHODAN Search Engine screenshot

Services

Service	Count
HTTP	6,692,080
HTTP Alternate	164,711
FTP	13,543
SNMP	9,022
UPnP	6,392

Top Countries

Country	Count
United States	3,352,389
China	506,298
United Kingdom	362,793
Germany	247,985
Canada	246,968

Top Cities

City	Count
Englewood	170,677
Beijing	111,663
Columbus	107,163
Dallas	90,899
Seoul	86,213

Top Organizations

Organization	Count
Verio Web Hosting	97,784
HiChina Web Solutions ...	52,629
Ecommerce Corporation	43,967
GoDaddy.com, LLC	33,234
Comcast Business Commu...	32,203

Error

66.77.20.147
Windows XP
Binnnews24.com
Added on 25.09.2012
Arlington
clients2.bn24.com

HTTP/1.0 403 Forbidden
Content-Length: 218
Content-Type: text/html
Server: Microsoft-IIS/6.0
IISExport: This web site was exported using IIS Export v4.1
X-Powered-By: ASP.NET
Date: Tue, 25 Sep 2012 01:53:00 GMT

www.net.cn

112.127.180.133
HiChina Web Solutions (Beijing) Limited
Added on 25.09.2012
Chaoyang

HTTP/1.0 200 OK
Content-Type: text/html
Last-Modified: Wed, 22 Jun 2011 10:28:46 GMT
Accept-Ranges: bytes
ETag: "083bd42ac730cc1:0"
Server: Microsoft-IIS/7.5
X-Powered-By: ASP.NET
X-UA-Compatible: IE=EmulateIE7
Date: Tue, 25 Sep 2012 01:53:02 GMT
Content-Length: 5304

The page must be viewed over a secure channel

41.216.174.82
Windows XP
VDT Communications Limited
Added on 25.09.2012
Wentworth Falls

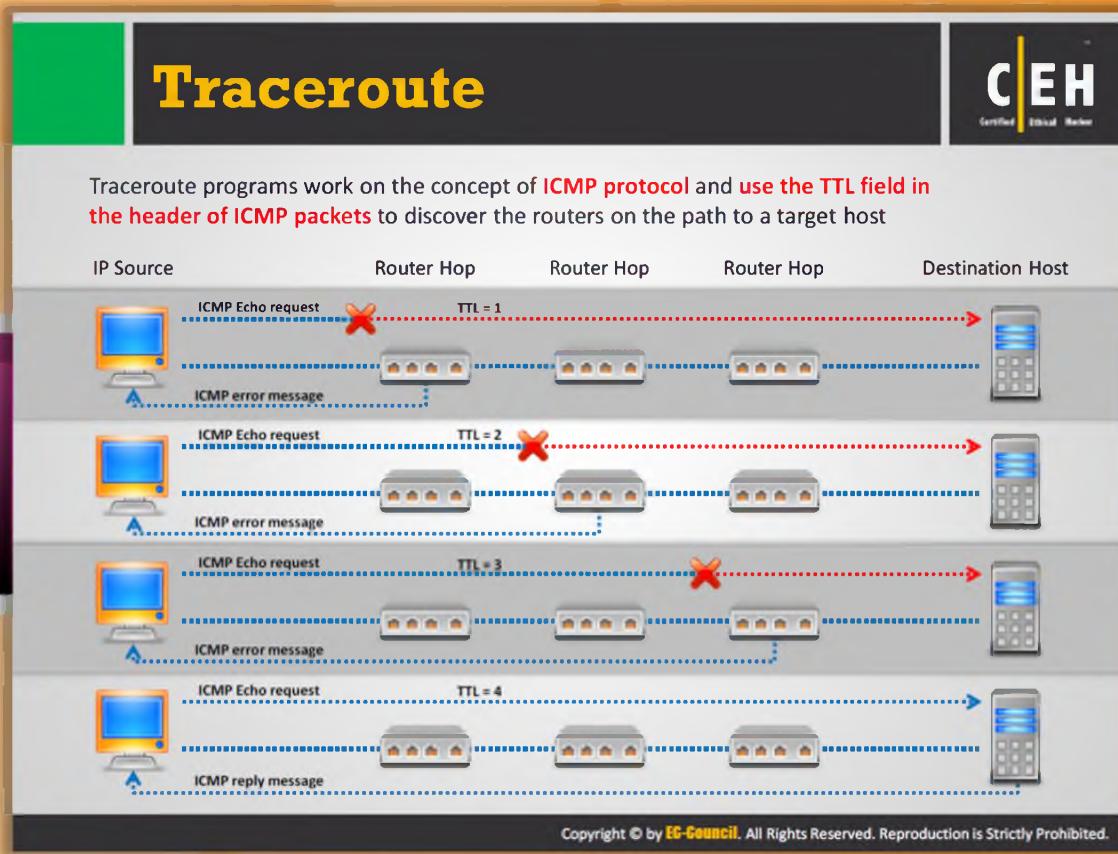
HTTP/1.0 403 Forbidden
Content-Length: 1409
Content-Type: text/html
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Date: Tue, 25 Sep 2012 01:59:20 GMT

IIS7

110.142.89.161
Telstra Internet
Added on 25.09.2012
Wentworth Falls

HTTP/1.0 200 OK
Content-Type: text/html
Last-Modified: Sat, 20 Nov 2010 03:13:31 GMT
Accept-Ranges: bytes
ETag: "3a24cbe86088cb1:0"
Server: Microsoft-IIS/7.5
X-Powered-By: ASP.NET
Date: Tue, 25 Sep 2012 01:52:50 GMT

FIGURE 2.35: SHODAN screenshot



Traceroute

Finding the route of the target host is necessary to test against **man-in-the-middle attacks** and other relative attacks. Therefore, you need to find the route of the target host in the network. This can be accomplished with the help of the Traceroute utility provided with most operating systems. It allows you to trace the path or route through which the target host packets travel in the network.

Traceroute uses the **ICMP protocol** concept and **TTL (Time to Live)** field of IP header to find the path of the target host in the network.

The Traceroute utility can detail the path IP packets travel between two systems. It can trace the number of routers the packets travel through, the round trip time duration in transiting between two routers, and, if the routers have DNS entries, the names of the routers and their network affiliation, as well as the geographic location. It works by exploiting a feature of the Internet Protocol called **Time To Live (TTL)**. The TTL field is interpreted to indicate the maximum number of routers a packet may transit. Each router that handles a packet will decrement the TTL count field in the ICMP header by one. When the count reaches zero, the packet will be discarded and an error message will be transmitted to the originator of the packet.

It sends out a packet destined for the destination specified. It sets the TTL field in the packet to one. The first router in the path receives the packet, decrements the TTL value by one, and if the resulting TTL value is 0, it discards the packet and sends a message back to the originating host to inform it that the packet has been discarded. It records the IP address and DNS name of that router, and sends out another packet with a TTL value of two. This packet makes it through the first router, then times-out at the next router in the path. This second router also sends an error message back to the originating host. Traceroute continues to do this, and records the IP address and name of each router until a packet finally reaches the target host or until it decides that the host is unreachable. In the process, it records the time it took for each packet to travel round trip to each router. Finally, when it reaches the destination, the normal ICMP ping response will be sent to the sender. Thus, this utility helps to reveal the IP addresses of the intermediate hops in the route of the target host from the source.

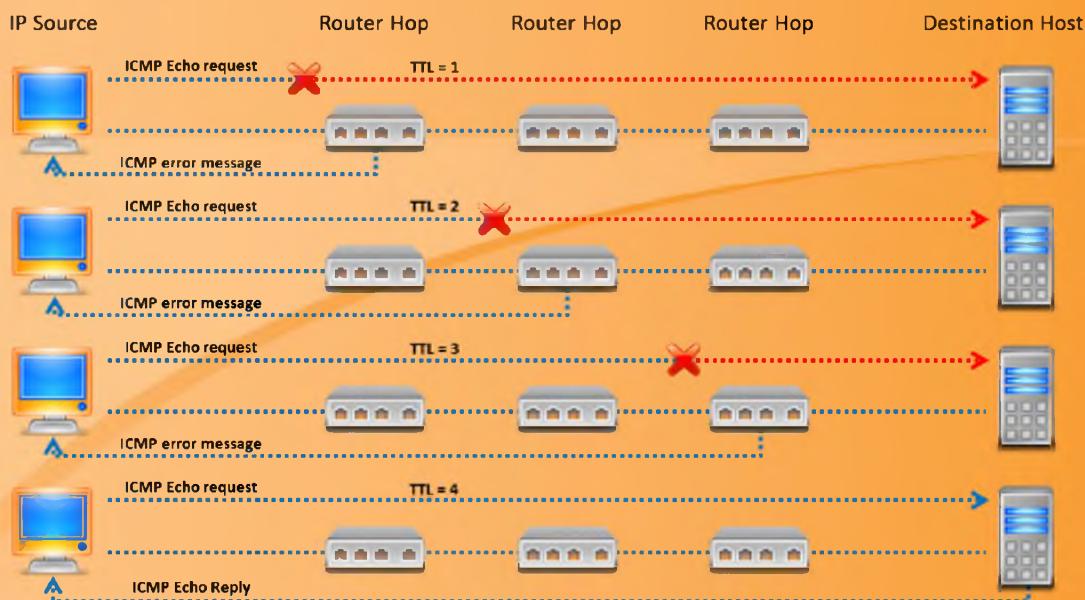


FIGURE 2.36: Working of Traceroute program

How to use the tracert command

Go to the command prompt and type the `tracert` command along with destination IP address or domain name as follows:

```
C:\>tracert 216.239.36.10
```

Tracing route to ns3.google.com [216.239.36.10] over a maximum of 30 hops:

```

1  1262 ms    186 ms    124 ms  195.229.252.10
2  2796 ms    3061 ms   3436 ms  195.229.252.130
3  155 ms     217 ms    155 ms  195.229.252.114
4  2171 ms    1405 ms   1530 ms  194.170.2.57
5  2685 ms    1280 ms    655 ms  dxb-emix-ra.ge6303.emix.ae [195.229.31.99]
6   202 ms     530 ms    999 ms  dxb-emix-rb.so100.emix.ae [195.229.0.230]
7   609 ms    1124 ms   1748 ms  iar1-so-3-2-0.Thameside.cw.net [166.63.214.65]
```

```
8 1622 ms 2377 ms 2061 ms eqixva-google-gige.google.com [206.223.115.21]
9 2498 ms 968 ms 593 ms 216.239.48.193
10 3546 ms 3686 ms 3030 ms 216.239.48.89
11 1806 ms 1529 ms 812 ms 216.33.98.154
12 1108 ms 1683 ms 2062 ms ns3.google.com [216.239.36.10]
```

Trace complete.

Traceroute Analysis

C|EH
Certified Ethical Hacker

- Attackers conduct traceroute to extract information about: **network topology, trusted routers, and firewall locations**
- For example: after running several **traceroutes**, an attacker might obtain the following information:
 - traceroute 1.10.10.20, second to last hop is 1.10.10.1
 - traceroute 1.10.20.10, third to last hop is 1.10.10.1
 - traceroute 1.10.20.10, second to last hop is 1.10.10.50
 - traceroute 1.10.20.15, third to last hop is 1.10.10.1
 - traceroute 1.10.20.15, second to last hop is 1.10.10.50
- By putting this information together, attackers can draw the **network diagram**

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



Traceroute Analysis

We have seen how the Traceroute utility helps you to find out the **IP addresses** of intermediate devices such as routers, firewalls, etc. present between source and destination. You can draw the network topology diagram by analyzing the **Traceroute results**. After running several traceroutes, you will be able to find out the location of a particular hop in the target network. Let's consider the following traceroute results obtained:

- traceroute 1.10.10.20, second to last hop is 1.10.10.1
- traceroute 1.10.20.10, third to last hop is 1.10.10.1
- traceroute 1.10.20.10, second to last hop is 1.10.10.50
- traceroute 1.10.20.15, third to last hop is 1.10.10.1
- traceroute 1.10.20.15, second to last hop is 1.10.10.50

By analyzing these results, an attacker can draw the network diagram of the target network as follows:

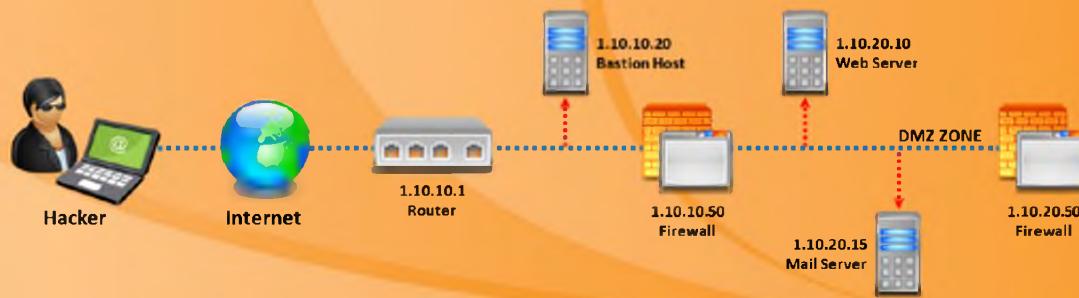


FIGURE 2.37: Diagrammatical representation of the target network



Traceroute Tools

Path Analyzer Pro and **VisualRoute 2010** are the two tools similar to Traceroute intended to traceroute the target host in a network.



Path Analyzer Pro

Source: <http://www.pathanalyzer.com>

Path Analyzer Pro is a **graphical-user-interface-based** trace routing tool that shows you the route from source to destination graphically. It also provides information such as the hop number, its IP address, hostname, ASN, network name, % loss, latency, avg. latency, and std. dev. about each hop in the path. You can also map the location of the IP address in the network with this tool. It allows you to detect filters, stateful firewalls, and other anomalies automatically in the network.

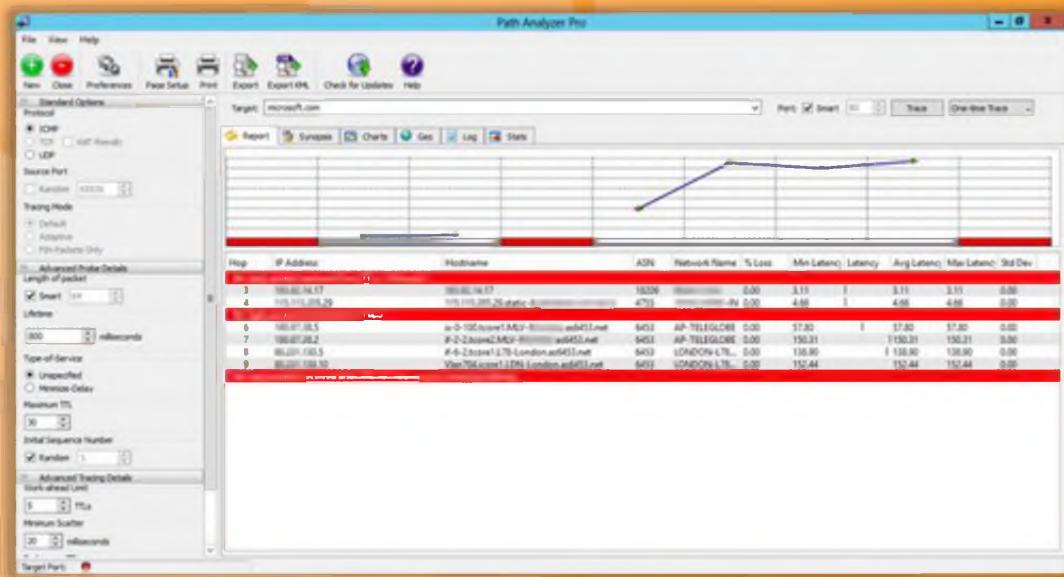


FIGURE 2.38: Path Analyzer Pro screenshot



VisualRoute 2010

Source: <http://www.visualroute.com>

This is another graphical-user-based tracing tool that displays **hop-by-hop analysis**. It enables you to identify the geographical location of the routers, servers, and other IP devices. It is able to provide the **tracing information** in three forms: as an overall analysis, in a data table, and as a geographical view of the routing. The data table contains information such as hop number, IP address, node name, geographical location, etc. about each hop in the route.

Features:

- ⊕ Hop-by-hop traceroutes
- ⊕ Reverse tracing
- ⊕ Historical analysis
- ⊕ Packet loss reporting
- ⊕ Reverse DNS
- ⊕ Ping plotting
- ⊕ Port probing
- ⊕ Firefox and IE plugin

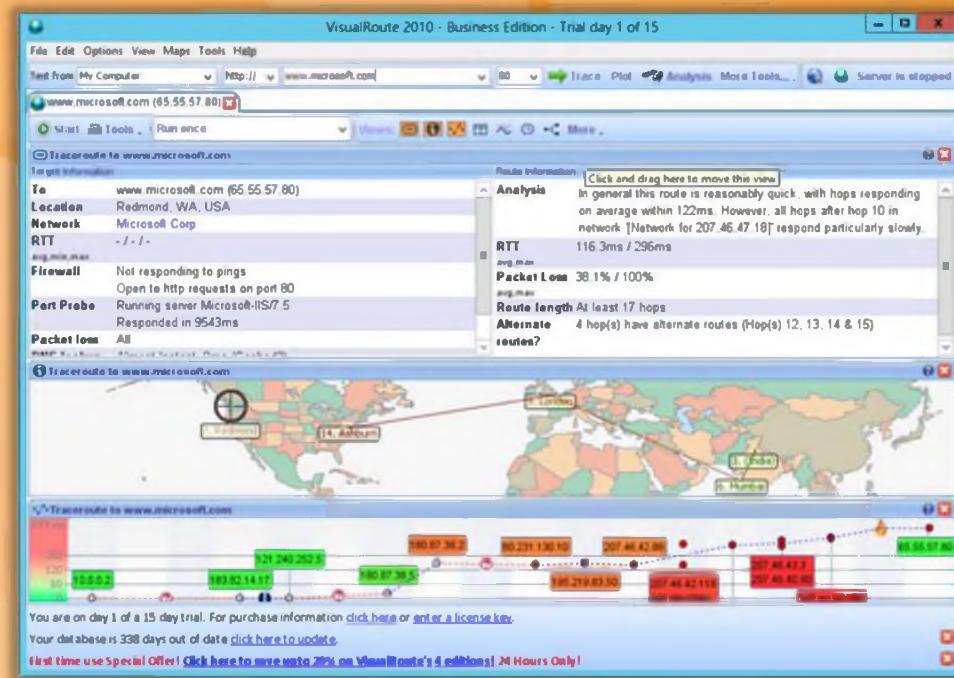


FIGURE 2.39: VisualRoute 2010 screenshot

Traceroute Tools (Cont'd)



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

 Network Pinger http://www.networkpinger.com	 Magic NetTrace http://www.tialsoft.com
 GEOSpider http://www.oreware.com	 3D Traceroute http://www.d3tr.de
 vTrace http://vtrace.pl	 AnalogX HyperTrace http://www.analogx.com
 Trout http://www.mcafee.com	 Network Systems Traceroute http://www.net.princeton.edu
 Roadkil's Trace Route http://www.roadkil.net	 Ping Plotter http://www.pingplotter.com

Traceroute Tools (Cont'd)

A few more traceroute tools similar to Path Analyzer Pro and VisualRoute 2010 are listed as follows:

- ⌚ Network Pinger available at <http://www.networkpinger.com>
- ⌚ GEOSpider available at <http://www.oreware.com>
- ⌚ vTrace available at <http://vtrace.pl>
- ⌚ Trout available at <http://www.mcafee.com>
- ⌚ Roadkil's Trace Route available at <http://www.roadkil.net>
- ⌚ Magic NetTrace available at <http://www.tialsoft.com>
- ⌚ 3D Traceroute available at <http://www.d3tr.de>
- ⌚ AnalogX HyperTrace available at <http://www.analogx.com>
- ⌚ Network Systems Traceroute available at <http://www.net.princeton.edu>
- ⌚ Ping Plotter available at <http://www.pingplotter.com>



Footprinting Methodology

So far we have discussed various techniques of gathering information either with the help of online resources or tools. Now we will discuss footprinting through **social engineering**, the art of grabbing information from people by manipulating them.

This section covers the social engineering concept and techniques used to gather information.

Footprinting through Social Engineering

C|EH
Certified Ethical Hacker

- Social engineering is the art of convincing people to reveal confidential information
- Social engineers depend on the fact that people are unaware of their valuable information and are careless about protecting it

Social engineers attempt to gather:

- Credit card details and social security number
- User names and passwords
- Other personal information
- Security products in use
- Operating systems and software versions
- Network layout information
- IP addresses and names of servers

Social engineers use these techniques:

- Eavesdropping
- Shoulder surfing
- Dumpster diving
- Impersonation on social networking sites

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



Footprinting through Social Engineering

Social engineering is a **totally non-technical process** in which an attacker tricks a person and obtains confidential information about the target in such a way that the target is unaware of the fact that someone is stealing his or her **confidential information**. The attacker actually plays a cunning game with the target to obtain confidential information. The attacker takes advantage of the helping nature of people and their weakness to provide confidential information.

To perform social engineering, you first need to **gain the confidence of an authorized user** and then trick him or her into revealing confidential information. The basic goal of social engineering is to obtain required confidential information and then use that information for hacking attempts such as gaining unauthorized access to the system, identity theft, industrial espionage, network intrusion, commit frauds, etc. The information obtained through social engineering may include credit card details, social security numbers, usernames and passwords, other personal information, operating systems and software versions, IP addresses, names of servers, network layout information, and much more. Social engineers use this information to hack a system or to commit fraud.

Social engineering can be performed in many ways such as **eavesdropping**, shoulder surfing, dumpster diving, impersonation on social networking sites, and so on.

Collect Information Using Eavesdropping, Shoulder Surfing, and Dumpster Diving



Eavesdropping

- Eavesdropping is **unauthorized listening of conversations** or reading of messages
- It is interception of any form of communication such as audio, video, or written

1



Shoulder Surfing

- Shoulder surfing is the procedure where the **attackers look over the user's shoulder** to gain critical information
- Attackers gather information such as passwords, personal identification number, account numbers, credit card information, etc.

2



Dumpster Diving

- Dumpster diving is **looking for treasure in someone else's trash**
- It involves collection of phone bills, contact information, financial information, operations related information, etc. from the target company's trash bins, printer trash bins, user desk for sticky notes, etc.

3

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



Collect Information using Eavesdropping, Shoulder Surfing, and Dumpster Diving

As mentioned previously eavesdropping, shoulder surfing, and dumpster driving are the three techniques used to collect information from people using social engineering. Let's discuss these social engineering techniques to understand how they can be performed to obtain confidential information.



Eavesdropping

Eavesdropping is the act of **secretly listening** to the conversations of people over a phone or videoconference without their consent. It also includes reading secret messages from communication media such as instant messaging or fax transmissions. Thus, it is basically the act of intercepting communication without the consent of the communicating parties. The attacker gains confidential information by tapping the phone conversation, and intercepting audio, video, or written communication.



Shoulder Surfing

With this technique, an **attacker stands** behind the victim and secretly observes the victim's activities on the computer such keystrokes while entering usernames, passwords, etc.

This technique is commonly used to gain passwords, PINs, security codes, account numbers, credit card information, and similar data. It can be performed in a crowded place as it is relatively easy to stand behind the victim without his or her knowledge.



Dumpster Diving

This technique is also known as **trashing**, where the attacker looks for information in the target company's dumpster. The attacker may **gain vital information** such as phone bills, contact information, financial information, operations-related information, printouts of source codes, printouts of sensitive information, etc. from the target company's trash bins, printer trash bins, and sticky notes at users' desks, etc. The obtained information can be helpful for the attacker to commit attacks.



Footprinting Methodology

Though footprinting through social networking sites sounds similar to **footprinting** through social engineering, there are some differences between the two methods. In footprinting through social engineering, the attacker tricks people into revealing information whereas in footprinting through social networking sites, the attacker gathers information available on social networking sites. Attackers can even use **social networking** sites as a medium to perform social engineering attacks.

This section explains how and what information can be collected from social networking sites by means of social engineering.

Collect Information through Social Engineering on Social Networking Sites

Attackers gather sensitive information through social engineering on social networking websites such as Facebook, MySpace, LinkedIn, Twitter, Pinterest, Google+, etc.

Attackers create a fake profile on social networking sites and then use the false identity to lure the employees to give up their sensitive information

Employees may post personal information such as date of birth, educational and employment backgrounds, spouses names, etc. and information about their company such as potential clients and business partners, trade secrets of business, websites, company's upcoming news, mergers, acquisitions, etc.

Using the details of an employee of the target organization, an attacker can compromise a secured facility

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

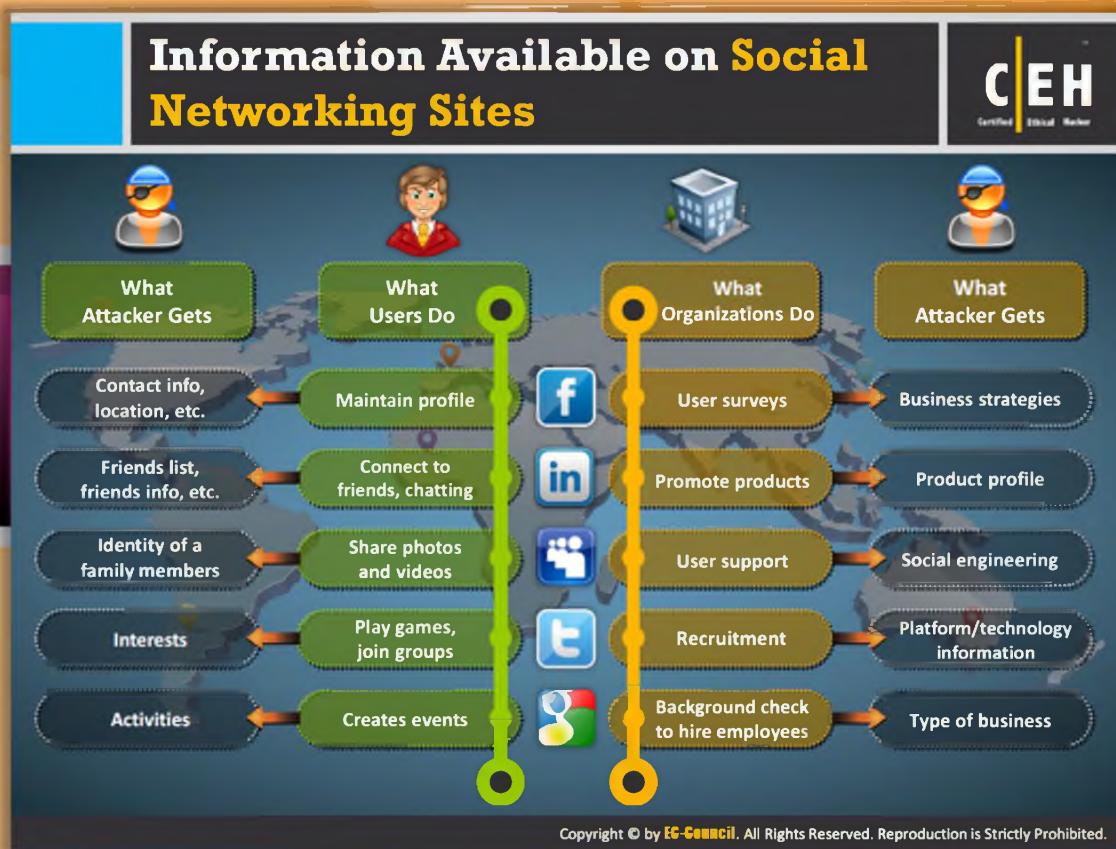


Collect Information through Social Engineering on Social Networking Sites

Social networking sites are the **online services**, platforms, or sites that allow people to connect with each other and to build social relations among people. The use of social networking sites is increasing rapidly. Examples of social networking sites include Facebook, MySpace, LinkedIn, Twitter, Pinterest, Google+, and so on. Each social networking site has its own purpose and features. One site may be intended to connect friends, family, etc. and another may be intended to share professional profiles, etc. These social networking sites are open to everyone. Attackers may take advantage of these to **grab sensitive information** from users either by browsing through users' public profiles or by creating a fake profile and tricking user to believe him or her as a genuine user. These **sites allow people** to stay connected with others, to maintain professional profiles, and to share the information with others. On social networking sites, people may post information such as date of birth, educational information, employment backgrounds, spouse's names, etc. and companies may post information such as potential partners, websites, and upcoming news about the company.

For an attacker, these **social networking sites** can be great sources to find information about the target person or the company. These sites help an attacker to collect only the information uploaded by the person or the company. Attackers can easily access public pages of these

accounts on the sites. To obtain more information about the target, attackers may create a fake account and use social engineering to lure the victim to reveal more information. For example, the attacker can send a friend request to the target person from the **fake account**; if the victim accepts the request, then the attacker can access even the restricted pages of the target person on that website. Thus, social networking sites prove to be a valuable information resource for attackers.



Information Available on Social Networking Sites

So far, we have discussed how an attacker can grab information from social networking sites; now we will discuss what information an attacker can get from social networking sites.

People usually maintain profiles on **social networking** sites in order to provide basic information about them and to get connected with others. The profile generally contains information such as name, contact information (mobile number, email ID), friends' information, information about family members, their interests, activities, etc. People usually connect to friends and chat with them. Attackers can gather sensitive information through their chats. Social networking sites also allow people to share photos and videos with their friends. If the people don't set their privacy settings for their **albums**, then **attackers** can see the pictures and videos shared by the victim. Users may join groups to play games or to share their views and interests. Attackers can **grab information** about a victim's interests by tracking their groups and then can trap the victim to reveal more information. Users may create events to notify other users of group about upcoming occasions. With these events, attackers can reveal the victim's activities. Like individuals, organizations also use social networking sites to connect with people, promote their products, and to gather feedback about their products or services, etc. The

activities of an organization on the social networking sites and the respective information that an **attacker** can grab are as follows:

What Organizations Do	What Attacker Gets
User surveys	Business strategies
Promote products	Product profile
User support	Social engineering
Background check to hire employees	Type of business

TABLE 2.1: What organizations Do and What Attacker Gets

Collecting Facebook Information

C|EH
Certified Ethical Hacker

Facebook is a Treasure-trove for Attackers

Number of users using Facebook all over the world

Category	Value
845 million monthly active users	845
100 billion connections	100
250 million photos uploaded daily	250
1 of every 5 of all page views	1/5
20 minutes time spent per visit	20

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



Collecting Facebook Information

Facebook is one of the **world's largest social networking sites**, having more than **845 million** monthly active users all over the world. It allows people to create their personal profile, add friends, exchange instant messages, create or join various groups or communities, and much more. An attacker can grab all the information provided by the victim on Facebook. To grab information from Facebook, the attacker should have an active account. The attacker should login to his/her account, and search for either the target person or **organization profile**. Browsing the target person's profile may reveal a lot of useful information such as phone number, email ID, friend information, educational details, professional details, his interests, photos, and much more. The attacker can use this information for further hacking planning, such as **social engineering**, to reveal more information about the target.



FIGURE 2.40: Facebook screenshot



Collecting Twitter Information

Twitter is another popular **social networking site** used by people to send and read **text-based messages**. It allows you to follow your friends, experts, favorite celebrities, etc. This site also can be a great source for an attacker to get information about the target person. This is helpful in extracting information such as personal information, friend information, activities of the target posted as tweets, whom the target is following, the followers of the user, **photos uploaded**, etc. The attacker may get meaningful information from the target user's tweets.

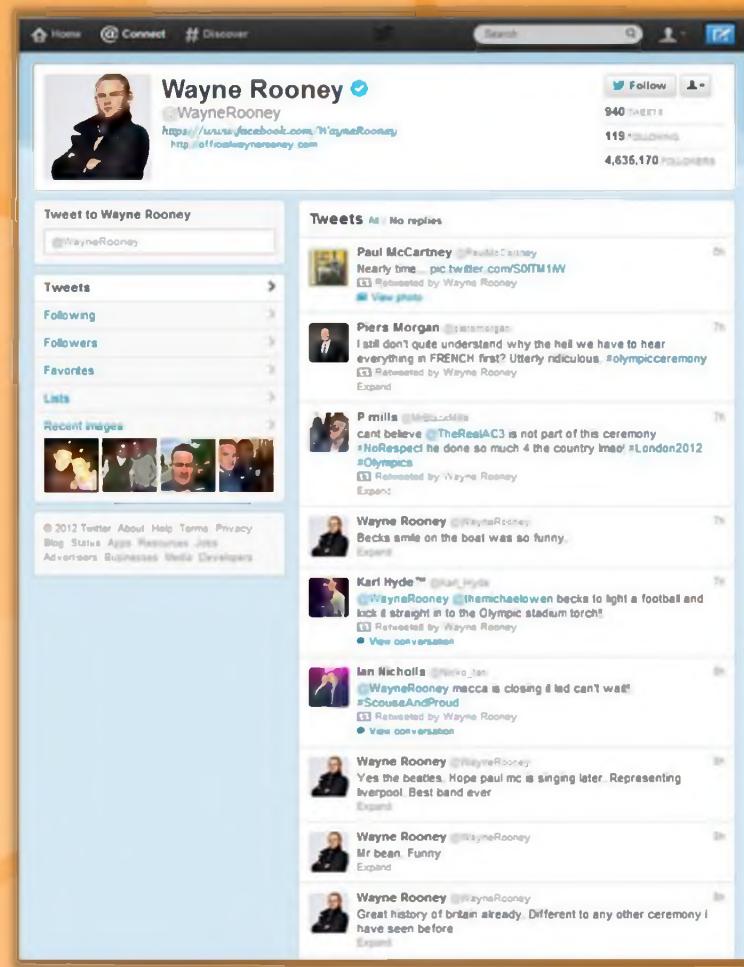


FIGURE 2.41: Twitter showing user's tweets

Collecting LinkedIn Information

C|EH
Certified Ethical Hacker

161 million members in over 200 countries

World map showing LinkedIn member counts by country:

- 6 million
- 2 million
- 4 million
- 4 million
- 57 million
- 4 million
- 2 million

LinkedIn Profile Example:

Chris Stone
Programmer Manager at Deutsche Bank AG
(Self-employed)
Past
Head of Operations - Products & Support, Investment Division at AAA
Programme Manager at AAA Bank Europe
Outsourcing Department & Procurement Manager at AAA
Education
Bachelor's Degree in Business Administration
Activities
1 group I have an interest in
Connections
100+ connections
Website
<http://bit.ly/ceh-linkedin-profile>

Key LinkedIn Statistics:

- 2 new members join every second**
- 2,447 employees located around the world**
- \$522 million revenue for 2011**
- 2 million companies have LinkedIn company pages**

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



Collecting LinkedIn Information

Similar to Facebook and Twitter, LinkedIn is another social networking site for professionals. It allows people to create and manage their **professional profile** and identity. It allows its users to build and engage with their professional network. Hence, this can be a great information resource for the attacker. The attacker may get information such as **current employment** details, past employment details, education details, contact details, and much more about the target person. The attacker can collect all this information with the **footprinting** process.

The screenshot shows a LinkedIn profile page for a user named Chris Stone. At the top, there's a navigation bar with links for Home, Profile, Contacts, Groups, Jobs, Inbox, Companies, News, and More. Below the navigation is a search bar with a 'People' dropdown and a 'Search' button.

The main content area displays the user's profile information:

- Profile Picture:** A small thumbnail of a man's face.
- Name:** Chris Stone
- Title:** Programme Manager at Deutsche Bank Belgium
- Location:** Brussels Area, Belgium | Management Consulting
- Current:** Programme Manager at Deutsche Bank Belgium
Director and Consultant at Program Management Solutions sprl
(Self-employed)
- Past:** Head of Operations, Projects & Support, Investment Division at AXA Bank Europe
Programme Manager at AXA Bank Europe
Outsourcing Programme & Procurement Manager at AXA Belgium □
see all □
- Education:** Henot-Watt
Institute of Chartered Secretaries and Administrators
- Recommendations:** 3 people have recommended Chris
- Connections:** 500+ connections
- Websites:** Company Website
- Public Profile:** <http://be.linkedin.com/in/cstone>

On the right side of the profile page, there are three buttons: 'See expanded', 'Connect', 'Send InMail', and 'Save Chris's Profile'.

FIGURE 2.42: LinkedIn showing user's professional profile and identity



Collecting YouTube Information

YouTube is a **website** that allows you to upload, view, and share videos all over the world. The attacker can search for the videos related to the target and may collect information from them.

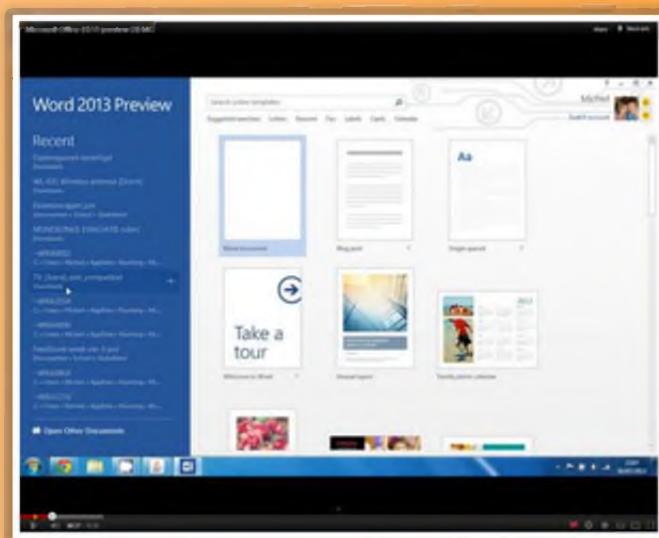


FIGURE 2.43: Youtube showing videos related to target

Tracking Users on Social Networking Sites

C|EH
Certified Ethical Hacker

- Users may use **fake identities** on social networking sites. Attackers use tools such as **Get Someones IP** or **IP-GRABBER** to track users' real identity
- Steps to get someone's IP address through chat on Facebook using **Get Someones IP** tool:
 - Go to <http://www.myiptest.com/staticpages/index.php/how-about-you>
 - Three fields exist:

Link for Person
Copy the **generated link** of this field and send it to the target via **chat** to get IP address

Redirect URL
Enter any **URL** you want the target to redirect to

Link for you
Open the **URL** in this field and keep checking for **target's IP**

Link for person: <http://www.myiptest.com/img.php?id=zdeujbg1f2&dmwww.gmail.com&ed=yahoo.com&>
Redirect URL: <http://www.gmail.com>
Link for you: http://www.myiptest.com/staticpages/index.php?how-about-you?id=zdeujbg1f2&show_ip

Link ID	IP	Proxy	Refer	Date/Time
zdeujbg1f2	85.93.218.204	NO	NO	2012-08-06 13:04:44

<http://www.myiptest.com>

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



Tracking Users on Social Networking Sites

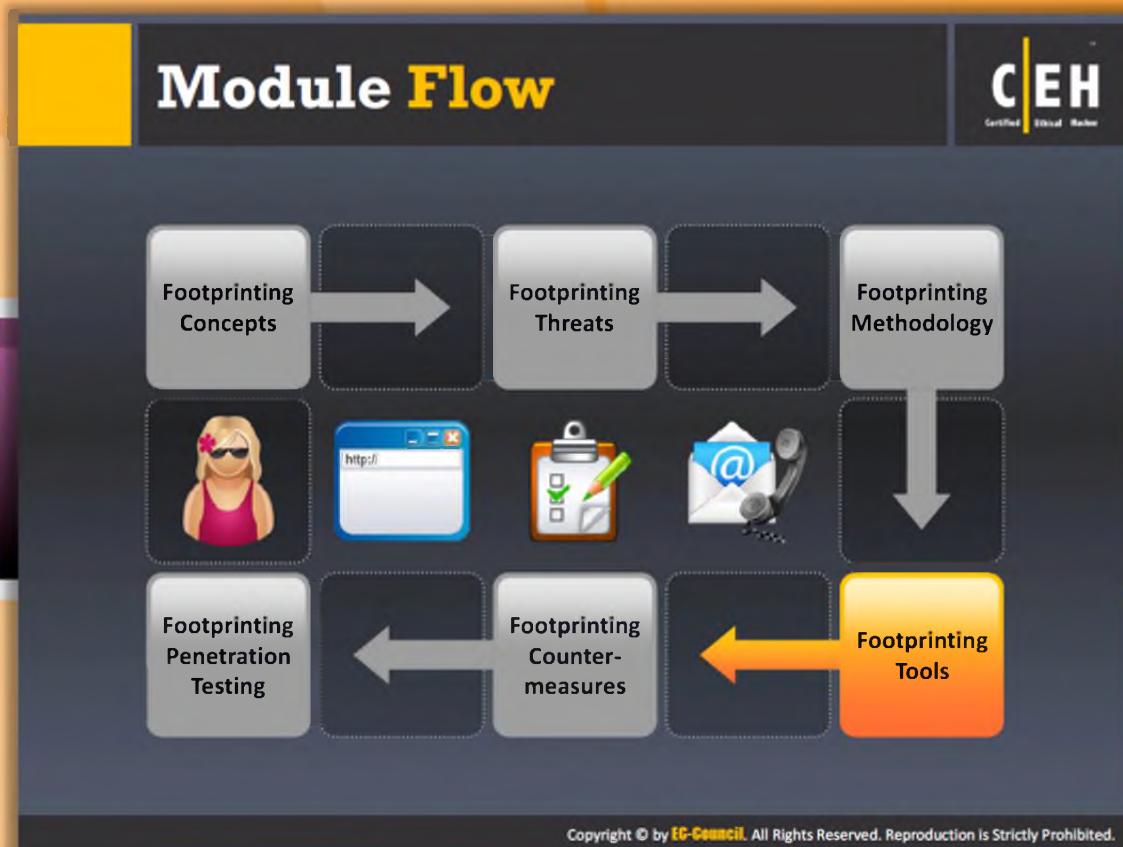
In order to protect themselves from **Internet fraud** and **attacks**, people with little knowledge about Internet crimes may use fake identities on social networking sites. In such cases, you will not get exact information about the target user. So to determine the real identity of the target user, you can use tools such as **Get Someone's IP** or **IP-GRABBER** to track users' real identities.

If you want to trace the identity of particular user, then do the following:

- Open your web browser, paste the URL, and press Enter:
<http://www.myiptest.com/staticpages/index.php/how-about-you>
- Notice the three fields at the bottom of the web page, namely **Link for person**, **Redirect URL**: <http://>, and **Link for you**.
 - To get real **IP address** of the target, copy the generated link of the **Link for person** field and send it to the target via chat.
 - Enter any **URL** you want the target to redirect to in the **Redirect link**: <http://> field.
 - Open the **URL** present in the **Link for you** field in another window, to monitor the target's IP address details and additional details.

Link for person:	http://www.myiptest.com/img.php?id=zdeujbg1f2&rdr=www.gmail.com&rdr=yahoo.com&			
Redirect URL:	http://www.gmail.com			
Link for you:	http://www.myiptest.com/staticpages/index.php/how-about-you?id=zdeujbg1f2&show_ip=1			
<hr/>				
Link ID	IP	Proxy	Refer	Date/Time
zdeujbg1f2	85.93.218.204	NO	NO	2012-08-06 13:04:44

FIGURE 2.44: Tracing identity of user's



Module Flow

Footprinting can be performed with the help of tools. Many organizations offer tools that make information gathering an easy job. These tools ensure the maximum

Footprinting Concepts	Footprinting Tools
Footprinting Threats	Footprinting Countermeasures
Footprinting Methodology	Footprinting Penetration Testing

This section describes tools intended for grabbing information from various sources.

Footprinting Tool: Maltego

C|EH
Certified Ethical Hacker

The image shows two screenshots of the Maltego application. The left screenshot displays a network graph for an 'Internet Domain', specifically for the URL <http://www.paterva.com>. The right screenshot shows a network graph for 'Personal Information'. Both interfaces feature a central workspace with nodes (represented by colored circles) connected by lines, surrounded by various toolbars and panels.

Maltego is a program that can be used to determine the **relationships and real world links** between people, groups of people (social networks), companies, organizations, websites, Internet infrastructure, phrases, documents, and files

Internet Domain
<http://www.paterva.com>

Personal Information

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



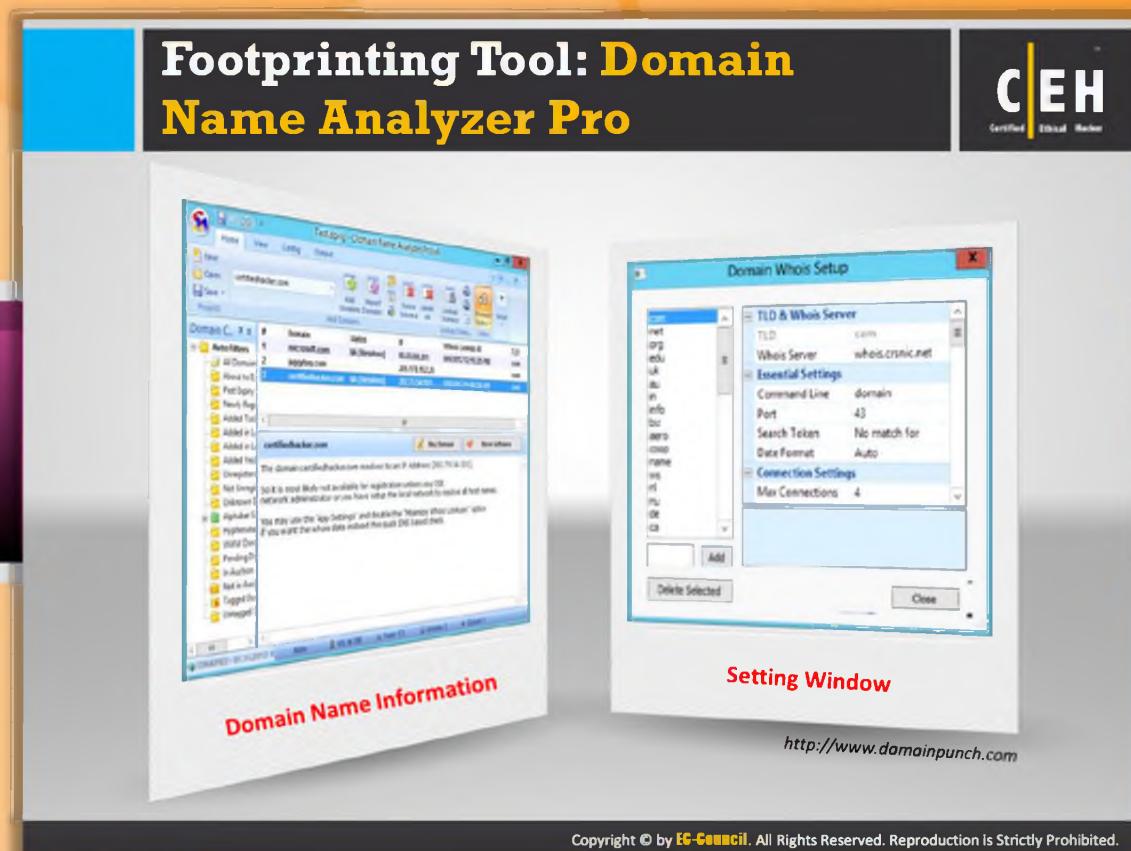
Footprinting Tool: Maltego

Source: <http://paterva.com>

Maltego is an open source **intelligence** and **forensics application**. It can be used for the information gathering phase of all **security-related work**. Maltego is a platform developed to deliver a clear threat picture to the environment that an organization owns and operates. It can be used to determine the relationships and real-world links between people, social networks, companies, organizations, websites, Internet infrastructure (domains, DNS names, Netblocks, IP addresses), phrases, affiliations, documents, and files.



FIGURE 2.45: Maltego showing Internet Domain and personal information

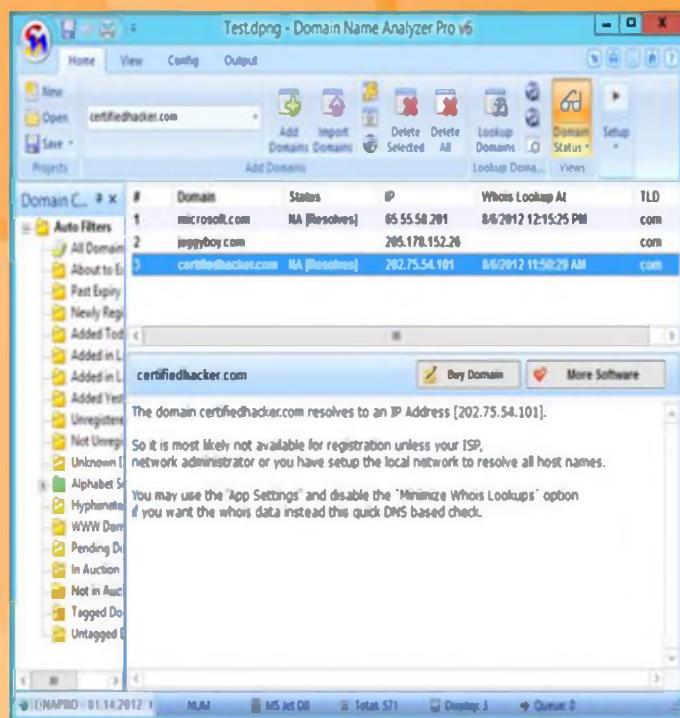


Footprinting Tool: Domain Name Analyzer Pro

Source: <http://www.domainpunch.com>

Domain Name Analyzer Professional is **Windows software** for finding, managing, and maintaining multiple domain names. It supports the display of additional data (expiry and creation dates, name server information), tagging domains, secondary whois lookups (for thin model whois TLDs like COM, NET, TV).

The following is a screenshot of the Domain Name **Analyzer Pro** tool showing domain name information:



Domain Name Information

FIGURE 2.46: Domain Name Analyzer Pro software showing Domain Name Information

The screenshot displays the Web Data Extractor software interface. At the top, there is a banner with the title "Footprinting Tool: Web Data Extractor" and the EC-Council Certified Ethical Hacker logo. Below the banner, two bullet points describe the tool's functions: "Extract targeted company contact data (email, phone, fax) from web for responsible b2b communication" and "Extract URL, meta tag (title, description, keyword) for website promotion, search directory creation, web research".

The main area contains three separate windows:

- Phone Numbers:** A table listing various phone numbers extracted from websites.
- Meta Tags:** A table listing extracted meta tags, including titles, descriptions, and keywords.
- Fax:** A table listing extracted fax numbers.

At the bottom of the interface, a copyright notice reads: "Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited."



Footprinting Tool: Web Data Extractor

Source: <http://www.webextractor.com>

Web Data Extractor is a **data extractor tool**. It extracts targeted company contact data (email, phone, and fax) from the web, extracts the **URL** and **meta tag** (title, desc, keyword) for website promotion, searches directory creation, etc. The following is a screenshot of the **Web Data Extractor** showing meta tags:

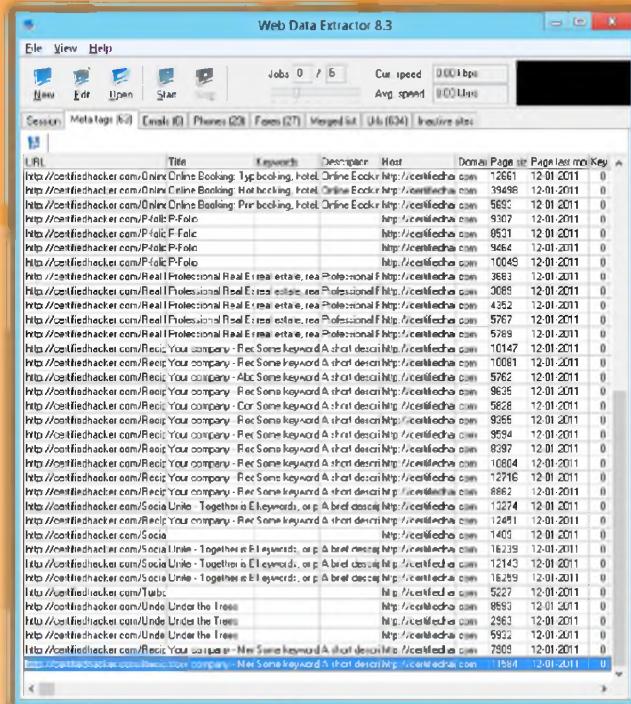


FIGURE 2.47: Web Data Extractor showing meta tags

Additional Footprinting Tools

C|EH
Certified Ethical Hacker

 Prefix Whois http://pwhois.org	 Netmask http://www.phenoelit-us.org
 NetScanTools Pro http://www.netscantools.com	 BingLNG http://www.blueinfy.com
 Tctrace http://www.phenoelit-us.org	 Spiderzilla http://spiderzilla.mozdev.org
 Autonomous System Scanner (ASS) http://www.phenoelit-us.org	 Sam Spade http://www.majorgeeks.com
 DNS DIGGER http://www.dnsdigger.com	 Robtex http://www.robtex.com

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



Additional Footprinting Tools

In addition to the footprinting tools mentioned previously, a few more tools are listed as follows:

- ⌚ Prefix Whois available at <http://pwhois.org>
- ⌚ NetScanTools Pro available at <http://www.netscantools.com>
- ⌚ Tctrace available at <http://www.phenoelit-us.org>
- ⌚ Autonomous System Scanner (ASS) available at <http://www.phenoelit-us.org>
- ⌚ DNS DIGGER available at <http://www.dnsdigger.com>
- ⌚ Netmask available at <http://www.phenoelit-us.org>
- ⌚ BingLNG available at <http://www.blueinfy.com>
- ⌚ Spiderzilla available at <http://spiderzilla.mozdev.org>
- ⌚ Sam Spade available at <http://www.majorgeeks.com>
- ⌚ Robtex available at <http://www.robtex.com>

Additional Footprinting Tools (Cont'd)


Certified Ethical Hacker

 Dig Web Interface http://www.digwebinterface.com	 SpiderFoot http://www.binarypool.com
 Domain Research Tool http://www.domainresearchtool.com	 CallerIP http://www.callerippro.com
 ActiveWhois http://www.johnru.com	 Zaba Search http://www.zabasearch.com
 yoName http://yename.com	 GeoTrace http://www.nabber.org
 Ping-Probe http://www.ping-probe.com	 DomainHostingView http://www.nirsoft.net

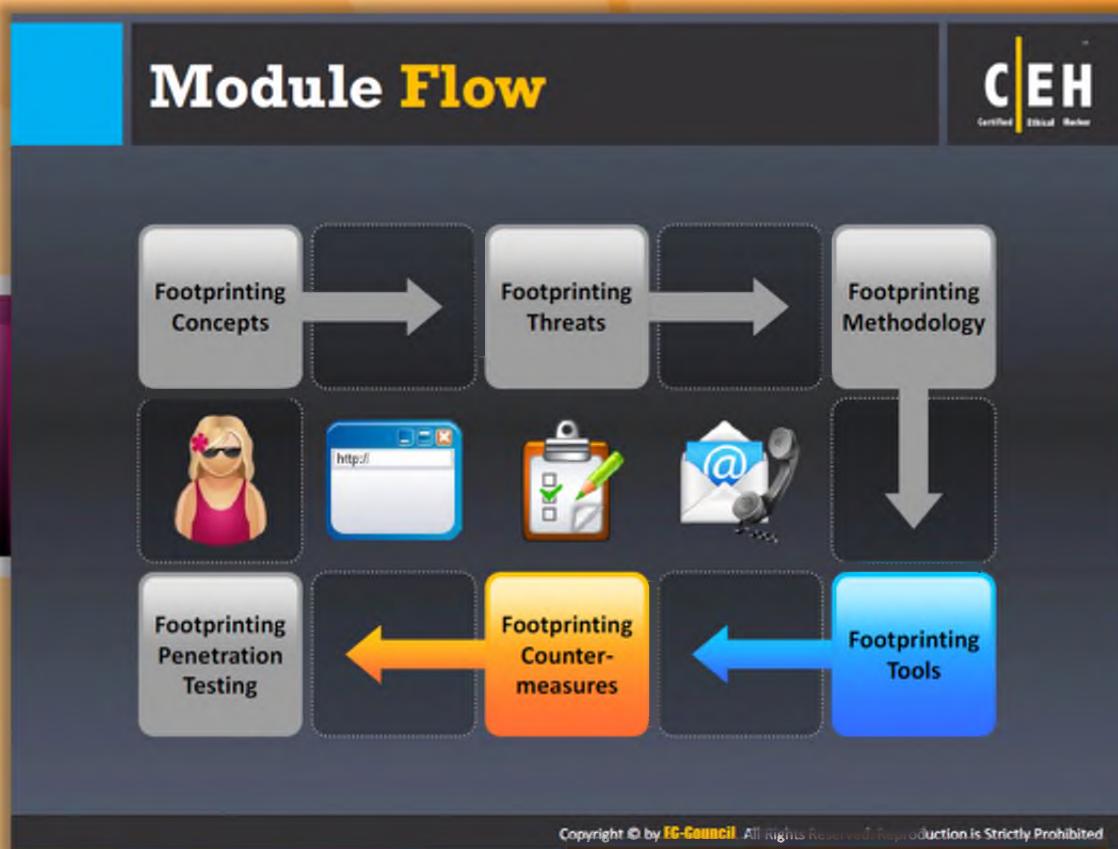
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



Additional Footprinting Tools (Cont'd)

Additional **footprinting** tools that are helpful in gathering information about the target person or organization are listed as follows:

- ⌚ Dig Web Interface available at <http://www.digwebinterface.com>
- ⌚ Domain Research Tool available at <http://www.domainresearchtool.com>
- ⌚ ActiveWhois available at <http://www.johnru.com>
- ⌚ yoName available at <http://yename.com>
- ⌚ Ping-Probe available at <http://www.ping-probe.com>
- ⌚ SpiderFoot available at <http://www.binarypool.com>
- ⌚ CallerIP available at <http://www.callerippro.com>
- ⌚ Zaba Search available at <http://www.zabasearch.com>
- ⌚ GeoTrace available at <http://www.nabber.org>
- ⌚ DomainHostingView available at <http://www.nirsoft.net>

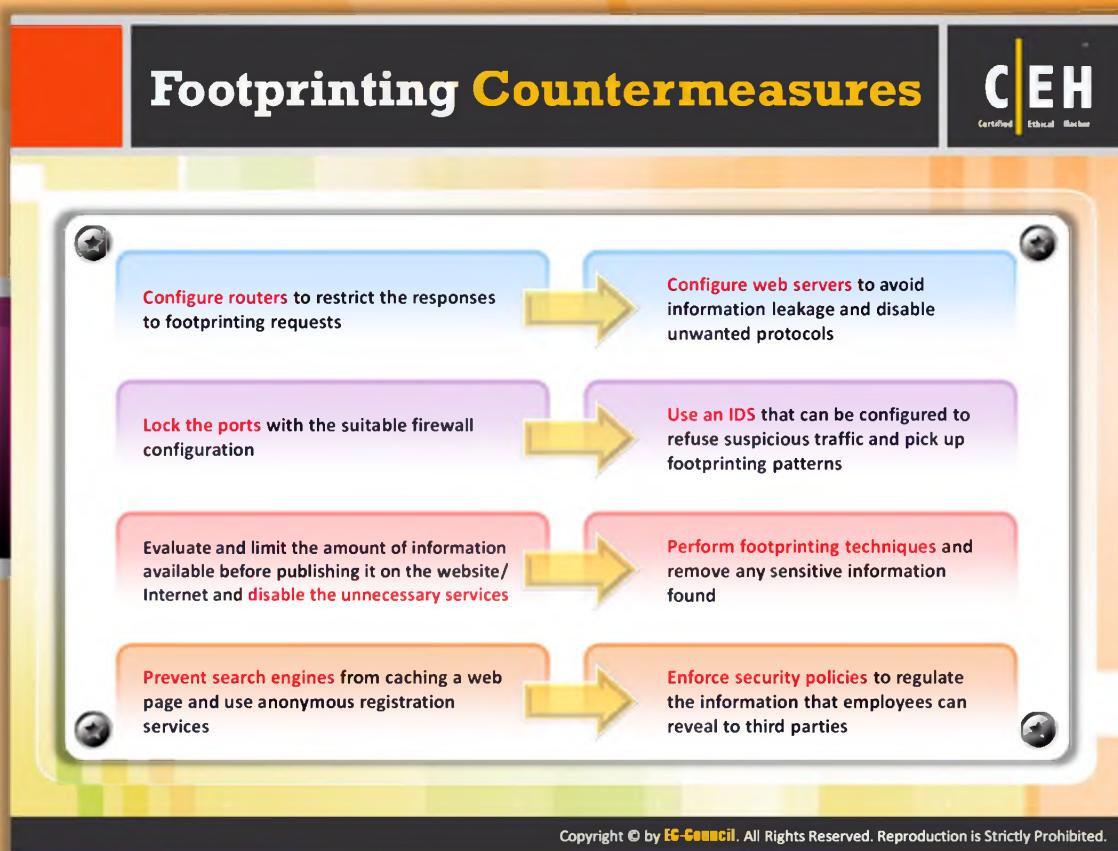


Module Flow

So far we have discussed the importance of footprinting, various ways in which footprinting can be performed, and the tools that can be used for footprinting. Now we will discuss the **countermeasures** to be applied in order to avoid sensitive information disclosure.

Footprinting Concepts	Footprinting Tools
Footprinting Threats	Footprinting Countermeasures
Footprinting Methodology	Footprinting Penetration Testing

This section lists various footprinting countermeasures to be applied at various levels.



Footprinting Countermeasures

Footprinting countermeasures are the measures or actions taken to counter or offset information disclosure. A few footprinting countermeasures are listed as follows:

- ⌚ Configure routers to restrict the responses to footprinting requests.
- ⌚ Lock the ports with suitable firewall configuration.
- ⌚ Evaluate and limit the amount of information available before publishing it on the **website/Internet** and disable the unnecessary services.
- ⌚ Prevent search engines from caching a webpage and use anonymous registration services.
- ⌚ Configure web servers to avoid information leakage and disable unwanted protocols.
- ⌚ Use an IDS that can be configured to refuse **suspicious traffic** and pick up footprinting patterns.
- ⌚ Perform footprinting techniques and remove any sensitive information found.
- ⌚ Enforce security policies to regulate the information that employees can reveal to third parties.

Footprinting Countermeasures (Cont'd)



Set apart internal DNS and external DNS

Disable directory listings and use split-DNS

Educate employees about various social engineering tricks and risks

Restrict unexpected input such as |; < >

Avoid domain-level cross-linking for the critical assets

Encrypt and password protect the sensitive information

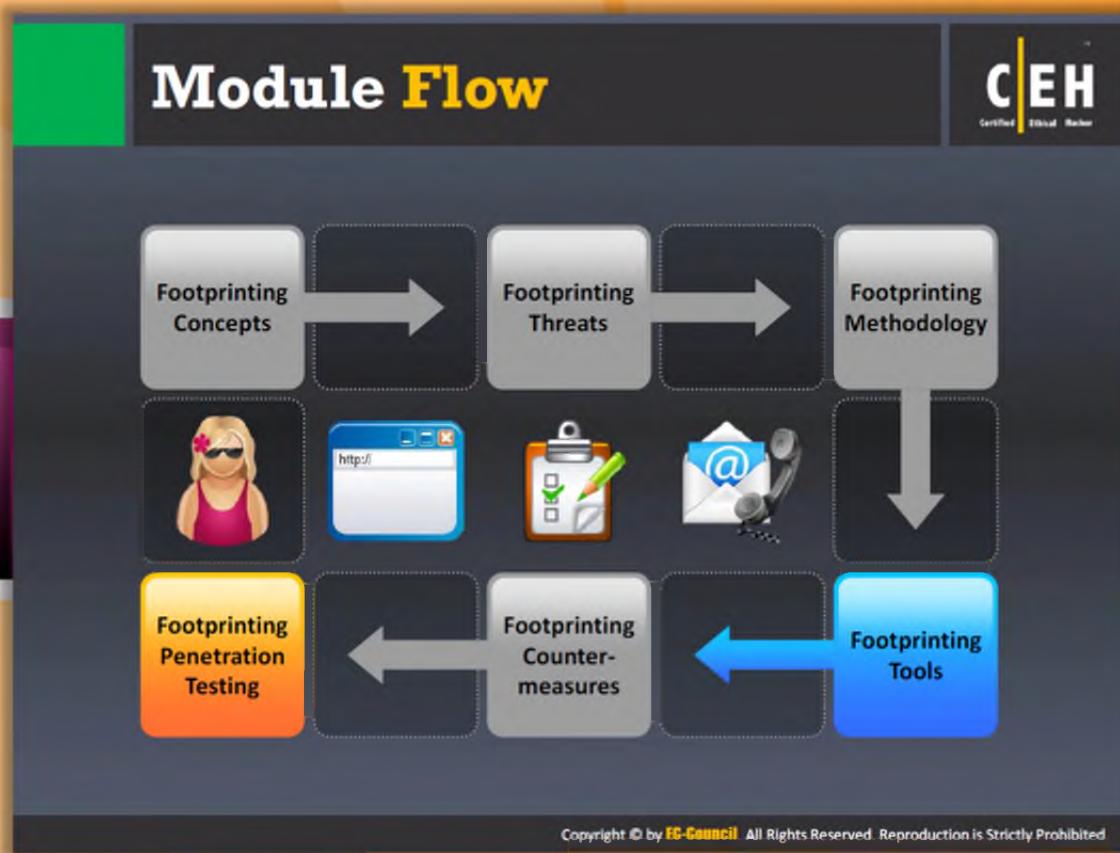
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



Footprinting Countermeasures (Cont'd)

In addition to the countermeasures mentioned previously, you can apply the following countermeasures as well:

- ➊ Set apart the internal DNS and external DNS.
- ➋ Disable directory listings and use split-DNS.
- ➌ Educate employees about various **social engineering tricks** and risks.
- ➍ Restrict unexpected input such as |; < >.
- ➎ Avoid domain-level cross-linking for critical assets.
- ➏ Encrypt and password protect sensitive information.
- ➐ Do not enable protocols that are not required.
- ➑ Always use TCP/IP and IPSec filters.
- ➒ Configure IIS against banner grabbing.



Module Flow

So far we discussed all the necessary techniques and tools to test the security of a system or network. Now it is the time to put all those **techniques** into practice. Testing the security of a system or network using similar techniques as that of an attacker with adequate permissions is known as **penetration testing**. The penetration test should be conducted to check whether an attacker is able to reveal sensitive information in response to footprinting attempts.

	Footprinting Concepts		Footprinting Tools
	Footprinting Threats		Footprinting Countermeasures
	Footprinting Methodology		Footprinting Penetration Testing

Penetration testing is an evaluation method of system or network security. In this evaluation method, the **pen tester** acts as a malicious outsider and simulates an attack to find the security loopholes.

Footprinting Pen Testing

C|EH
Certified Ethical Hacker

- Footprinting pen test is used to determine **organization's publicly available information on the Internet** such as network architecture, operating systems, applications, and users
- The tester attempts to gather as much information as possible about the target organization from the **Internet and other publicly accessible sources**

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

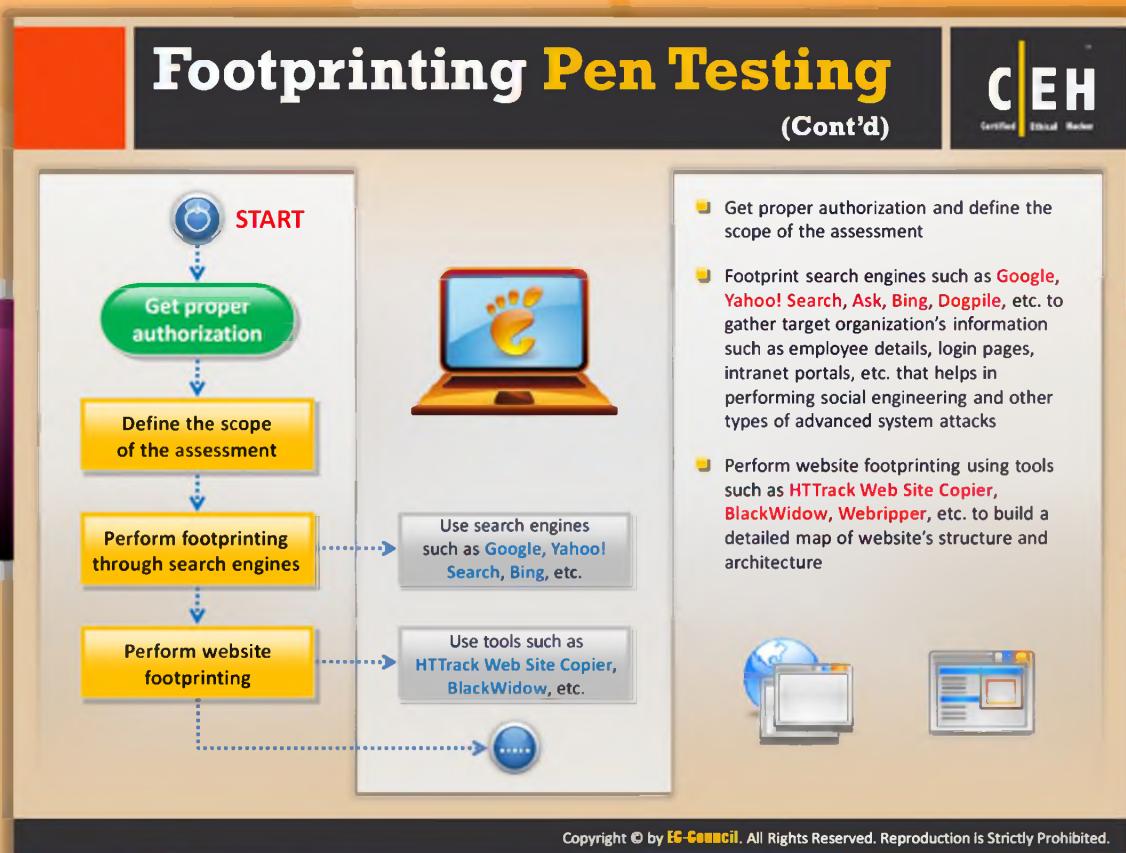
Footprinting Pen Testing

A footprinting pen test is used to determine an organization's publicly available **information on the Internet** such as network architecture, operating systems, applications, and users. In this method, the pen tester tries to gather publicly available sensitive information of the target by pretending to be an attacker. The target may be a specific host or a network.

The pen tester can perform any attack that an attacker could perform. The pen tester should try all possible ways to gather as much information as possible in order to ensure maximum scope of footprinting pen testing. If the pen tester finds any **sensitive information** on any publicly available information resource, then he or she should enter the information and the respective source in the report.

The major advantages of conducting penetration testing include:

- It gives you the chance to prevent DNS record retrieval from publicly available servers.
- It helps you to avoid information leakage.
- It prevents **social engineering** attempts.



Footprinting Pen Testing (Cont'd)

Penetration testing is a procedural way of testing the security in various steps. Steps should be followed one after the other in order to ensure **maximum scope** of testing. Here are the steps involved in footprinting pen testing:

Step 1: Get proper authorization

Pen testing should be **performed with permission**. Therefore, the very first step in a footprinting pen test is to get proper authorization from the concerned people, such as administrators.

Step 2: Define the scope of the assessment

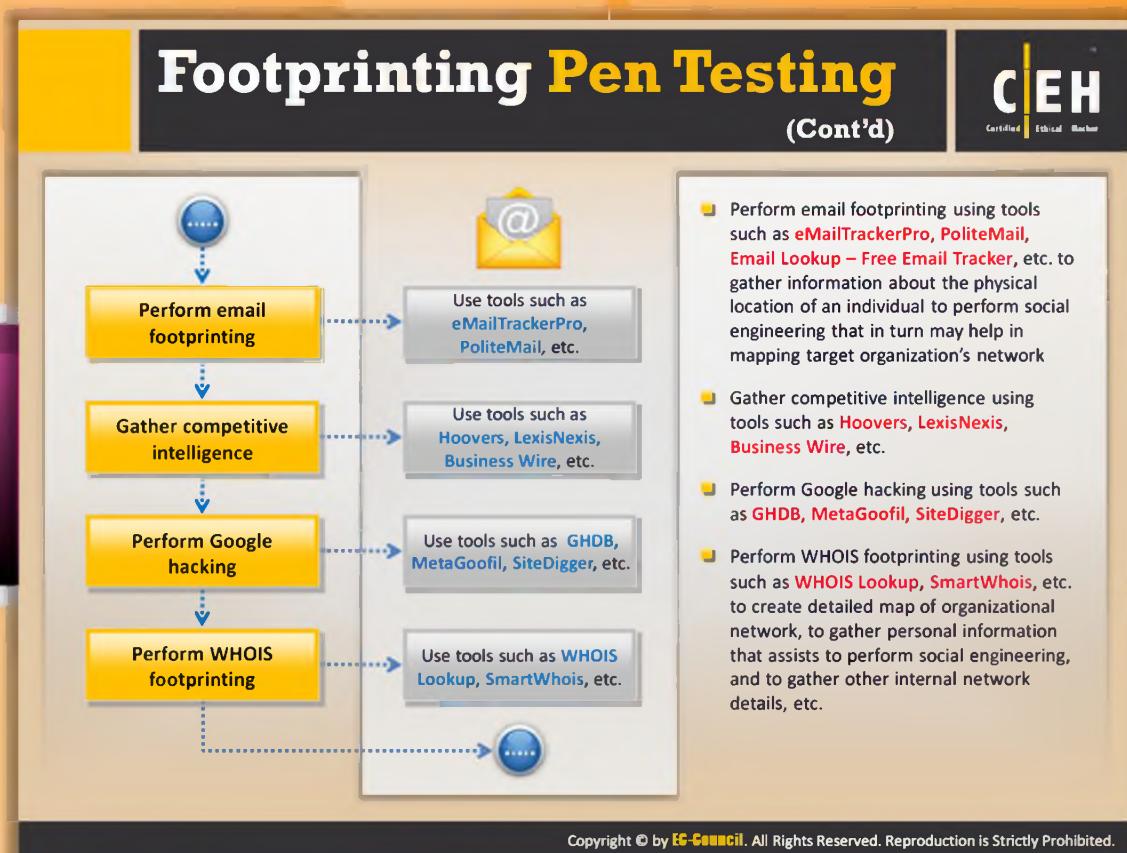
Defining the scope of the **security assessment** is the prerequisite for penetration testing. Defining the scope of assessment determines the range of systems in the network to be tested and the resources that can be used to test, etc. It also determines the pen tester's limitations. Once you define the scope, you should plan and gather sensitive information using various footprinting techniques.

Step 3: Perform footprinting through search engines

Footprint search engines such as Google, Yahoo! Search, Ask, Bing, Dogpile, etc. to gather the target organization's information such as employee details, login pages, intranet portals, etc. that can help in performing social engineering and other types of **advanced system attacks**.

Step 4: Perform website footprinting

Perform website footprinting using tools such as HTTrack Web Site Copier, BlackWidow, Webripper, etc. to build a detailed map of the **website's structure and architecture**.



Footprinting Pen Testing (Cont'd)

Step 5: Perform email footprinting

Perform email footprinting using tools such as eMailTrackerPro, PoliteMail, Email Lookup – Free Email Tracker, etc. to gather information about the physical location of an individual to perform **social engineering** that in turn may help in mapping the target organization's network.

Step 6: Gather competitive intelligence

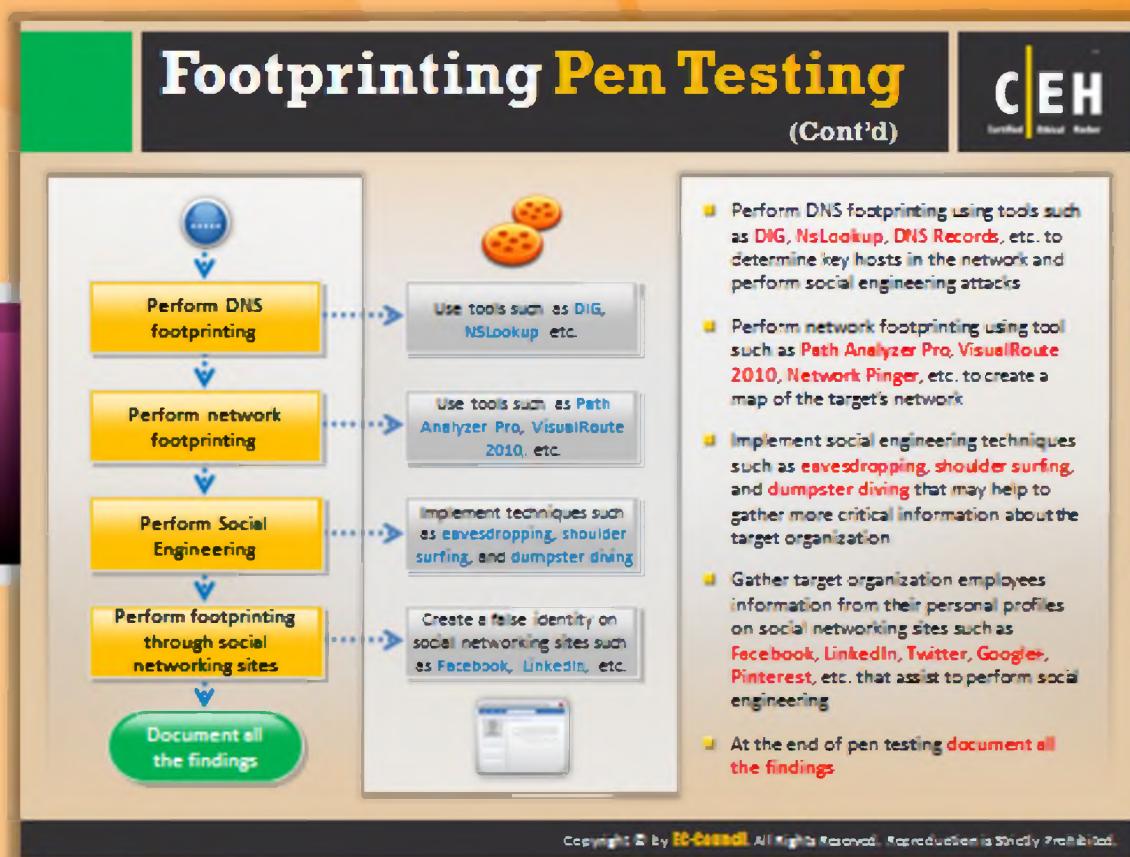
Gather competitive intelligence using tools such as **Hoovers**, SEC Info, Business Wire, etc. These tools help you to extract a competitor's information such as its establishment, location of the company, progress analysis, higher authorities, product analysis, marketing details, and much more.

Step 7: Perform Google hacking

Perform Google hacking using tools such as GHDB, MetaGoofil, SiteDigger, etc. It determines the **security loopholes** in the code and configuration of the websites. Google hacking is usually done with the help of advanced Google operators that locate specific strings of text such as versions of vulnerable web applications.

Step 8: Perform WHOIS footprinting

Perform the WHOIS **footprinting technique** to extract information about particular domains. You can get information such as domain name, IP address, domain owner name, registrant name, and their contact details including phone numbers, email IDs, etc. Tools such as SmartWhois, CountryWhois, Whois Pro, and ActiveWhois will help you to extract this information. You can use this information to perform **social engineering** to obtain more information.



Footprinting Pen Testing (Cont'd)

Step 9: Perform DNS footprinting

Perform DNS footprinting using tools such as DIG, NsLookup, DNS Records, etc. to determine key hosts in the network and perform **social engineering attacks**. Resolve the domain name to learn about its IP address, DNS records, etc.

Step 11: Perform network footprinting

Perform network footprinting using tools such as Path Analyzer Pro, VisualRoute 2010, Network Pinger, etc. to create a map of the target's network. Network footprinting allows you to reveal the network range and other **network information** of the target network. Using all this information, you can draw the network diagram of the target network.

Step 12: Perform social engineering

Implement social engineering techniques such as **eavesdropping**, **shoulder surfing**, and **dumpster diving** that may help to gather more critical information about the target organization. Through social engineering you can gather **target organization's** employee details, phone numbers, contact address, email address, etc. You can use this information to reveal even more information.

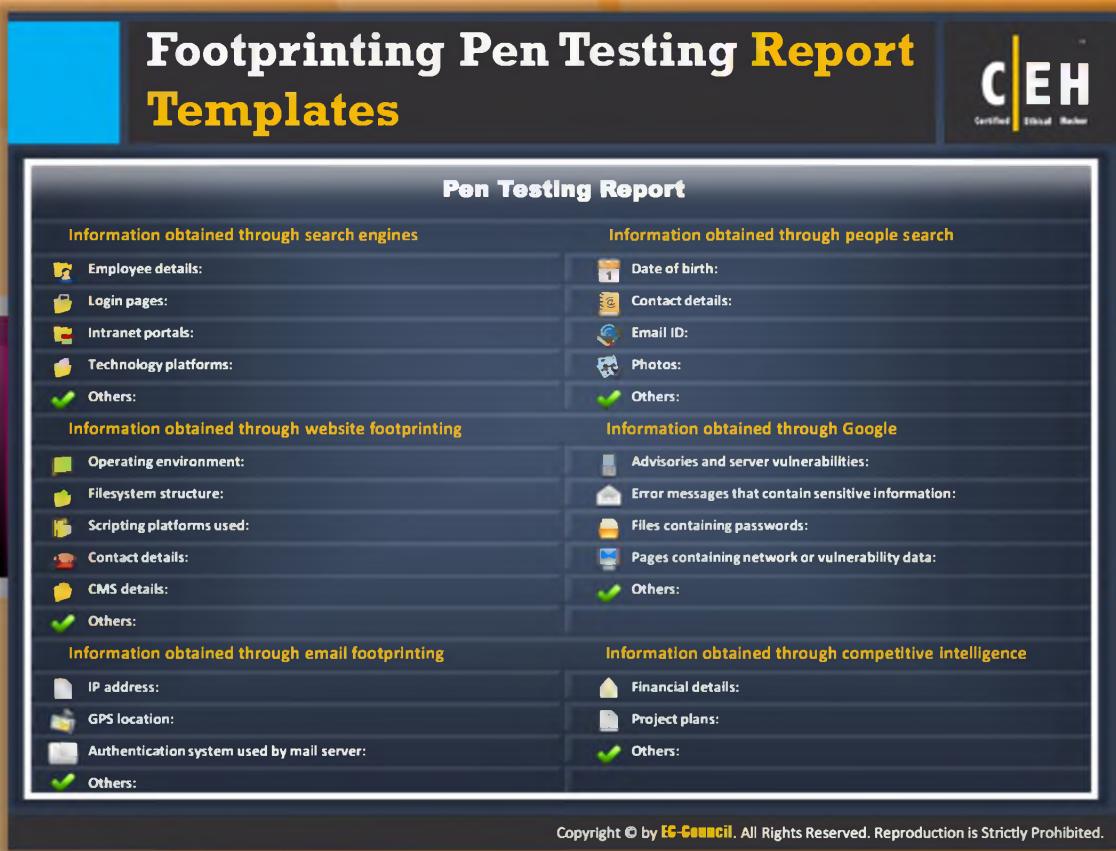
Step 13: Perform footprinting through social networking sites

Perform footprinting through social networking sites on the employees of the **target organization** obtained in footprinting through social engineering. You can gather information from their personal profiles on social networking sites such as Facebook, LinkedIn, Twitter, Google+, Pinterest, etc. that assists in **performing social engineering**. You can also use people search engines to obtain information about target person.

Step 14: Document all the findings

After implementing all the **footprinting techniques**, collect and document all the information obtained at every stage of testing. You can use this document to study, understand, and analyze the security posture of the target organization. This also enables you to find security loopholes. Once you find security loopholes, you should suggest respective countermeasures to the loopholes.

The following is a summary of footprinting **penetration testing**.



The image shows a template for a 'Footprinting Pen Testing Report Templates'. The header features the 'CEH' logo with 'Certified Ethical Hacker' underneath. The main section is titled 'Pen Testing Report' and is divided into several categories of information obtained through various methods:

- Information obtained through search engines**: Employee details, Login pages, Intranet portals, Technology platforms, Others.
- Information obtained through people search**: Date of birth, Contact details, Email ID, Photos, Others.
- Information obtained through website footprinting**: Operating environment, Filesystem structure, Scripting platforms used, Contact details, CMS details, Others.
- Information obtained through Google**: Advisories and server vulnerabilities, Error messages that contain sensitive information, Files containing passwords, Pages containing network or vulnerability data, Others.
- Information obtained through email footprinting**: IP address, GPS location, Authentication system used by mail server, Others.
- Information obtained through competitive intelligence**: Financial details, Project plans, Others.

At the bottom, a copyright notice reads: Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Footprinting Pen Testing Report Templates



Pen Testing Report

Penetration testing is usually conducted to enhance the **security perimeter** of an organization. As a pen tester you should gather sensitive information such as server details, the operating system, etc. of your target by conducting footprinting. Analyze the system and network defenses by breaking into its security with **adequate permissions** (i.e., ethically) without causing any damage. Find the loopholes and weaknesses in the network or system security. Now explain all the **vulnerabilities** along with respective countermeasures in a report, i.e., the pen testing report. The pen testing report is a report obtained after performing network penetration tests or security audits. It contains all the details such as types of tests performed, the **hacking techniques** used, and the results of hacking activity. In addition, the report also contains the highlights of security risks and vulnerabilities of an organization. If any vulnerability is identified during any test, the details of the cause of vulnerability along with the countermeasures are suggested. The report should always be kept **confidential**. If this information falls into the hands of attacker, he or she may use this information to launch attacks.

The pen testing report should contain the following details:

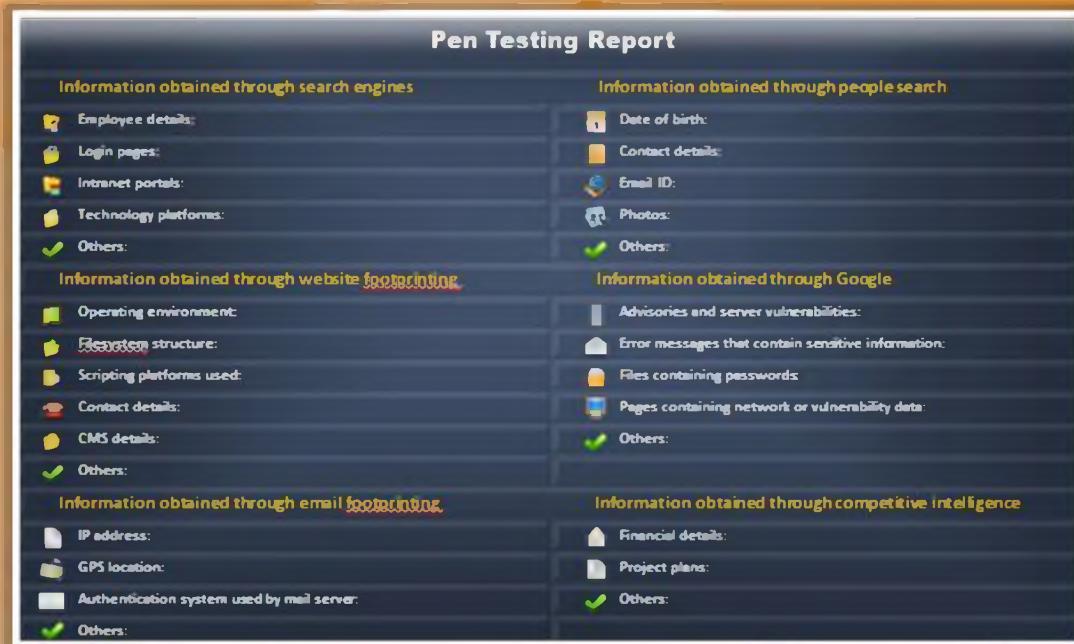


FIGURE 2.48: Pen Testing Report

Footprinting Pen Testing Report Templates (Cont'd)

Pen Testing Report

Information obtained through WHOIS footprinting

- Domain name details:
- Contact details of domain owner:
- Domain name servers:
- Netrange:
- When a domain has been created:
- Others:**

Information obtained through DNS footprinting

- Location of DNS servers:
- Type of servers:
- Others:**

Information obtained through network footprinting

- Range of IP addresses:
- Subnet mask used by the target organization:
- OS's in use:
- Firewall locations:
- Others:**

Information obtained through social engineering

- Personal information:
- Financial information:
- Operating environment:
- User names and passwords:
- Network layout information:
- IP addresses and names of servers:
- Others:**

Information obtained through social networking sites

- Personal profiles:
- Work related information:
- News and potential partners of the target company:
- Educational and employment backgrounds:
- Others:**

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

Footprinting Pen Testing Report Templates (Cont'd)

Pen Testing Report

Information obtained through WHOIS footprinting

- Domain name details:
- Contact details of domain owner:
- Domain name servers:
- Netrange:
- When a domain has been created:
- Others:**

Information obtained through DNS footprinting

- Location of DNS servers:
- Type of servers:
- Others:**

Information obtained through network footprinting

- Range of IP addresses:
- Subnet mask used by the target organization:
- OS's in use:
- Firewall locations:
- Others:**

Information obtained through social engineering

- Personal information:
- Financial information:
- Operating environment:
- Usernames and passwords:
- Network layout information:
- IP addresses and names of servers:
- Others:**

Information obtained through social networking sites

- Personal profiles:
- Work related information:
- News and potential partners of the target company:
- Educational and employment backgrounds:
- Others:**

FIGURE 2.49: Pen Testing Report showing information obtained through footprinting and social engineering

Module Summary



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

- ❑ Footprinting is the process of collecting as much information as possible about a target network, for identifying various ways to intrude into an organization's network system
- ❑ It reduces attacker's attack area to specific range of IP address, networks, domain names, remote access, etc.
- ❑ Attackers use search engines to extract information about a target
- ❑ Information obtained from target's website enables an attacker to build a detailed map of website's structure and architecture
- ❑ Competitive intelligence is the process of identifying, gathering, analyzing, verifying, and using information about your competitors from resources such as the Internet
- ❑ DNS records provide important information about location and type of servers
- ❑ Attackers conduct traceroute to extract information about: network topology, trusted routers, and firewall locations
- ❑ Attackers gather sensitive information through social engineering on social networking websites such as Facebook, MySpace, LinkedIn, Twitter, Pinterest, Google+, etc.



Module Summary

- ➊ Footprinting refers to uncovering and collecting as much information as possible about a target of attack.
- ➋ It reduces attacker's attack area to specific range of IP address, networks, domain names, remote access, etc.
- ➌ Attackers use search engines to extract information about a target.
- ➍ Information obtained from target's website enables an attacker to build a detailed map of website's structure and architecture.
- ➎ Competitive intelligence is the process of identifying, gathering, analyzing, verifying, and using information about your competitors from resources such as the Internet.
- ➏ DNS records provide important information about location and type of servers.
- ➐ Attackers conduct traceroute to extract information about: network topology, trusted routers, and firewall locations.
- ➑ Attackers gather sensitive information through social engineering on social networking websites such as Facebook, MySpace, LinkedIn, Twitter, Pinterest, Google+, etc.

Scanning Networks

Module 03



Ethical Hacking and Countermeasures v8

Module 03: Scanning Networks

Exam 312-50

The screenshot shows a news article from a website. At the top, there's a yellow header bar with the text "Security News". To the right of the header is a logo for "CEH Certified Ethical Hacker". Below the header, there's a navigation menu with links for Home, Services, Company, Networks, and Contact. The date "Oct 18 2012" is displayed. The main title of the article is "Saliently Sality Botnet Trapped Scanning IPv4 Address Space". The article content discusses the Sality botnet, which scans the entire IPv4 address space without alerts. It mentions that Sality is malware used for infecting web servers, dispersing spam, and stealing data. The article also notes that it uses reverse-byte order scanning and that target IP addresses are selected in reverse-byte-order increments. A link to the source "http://www.spamfighter.com" is provided at the bottom of the article.



Security News

Saliently Sality Botnet Trapped Scanning IPv4 Address Space

Source: <http://www.spamfighter.com>

A semi-famous botnet, Sality, used for locating vulnerable **voice-over-IP (VoIP)** servers has been controlled toward determining the entire **IPv4 address space** without setting off alerts, claims a new study, published by Paritynews.com, on October 10, 2012.

Sality is a piece of malware with the primary aim of infecting web servers, **dispersing** spam, and **stealing data**. But the latest research has disclosed other purposes, including recognizing susceptible VoIP targets that could be used in toll fraud attacks.

Through a method called "**reverse-byte order scanning**," Sality can be administered toward scanning possibly the whole IPv4 space, devoid of being recognized. That's the only reason the technique uses a very small number of packets that come from various sources.

The selection of the target IP addresses develops in **reverse-byte-order increments**. Also, there are many bots contributing in the scan. The conclusion is that a solitary network would obtain scanning packets "**diluted**" over a huge period of time (12 days in this case, from various

sources, **University of California, San Diego (UCSD)**, claimed one of the researchers, Alistair King, as published by Softpedia.com on October 9, 2012).

According to **Alberto Dainotti**, it's not that this stealth-scanning method is exceptional, but it's the first time that such a happening has been both noticed and documented, as reported by Darkreading.com on October 4, 2012. Many other experts hold faith that this manner has been accepted by other botnets. Nevertheless, the team at UCSD is not aware of any data verifying any event like this one.

According to **David Piscitello**, Senior Security Technologist at ICANN, this indeed seems to be the first time that researchers have recognized a botnet that utilizes this scanning method by employing reverse-byte sequential increments of target IP addresses. The **botnet** use classy "**orchestration**" methods to **evade detection**. It can be simply stated that the botnet operator categorized the scans at around **3 million bots** for scanning the full IPv4 address space through a scanning pattern that disperses coverage and partly covers, but is unable to be noticed by present automation, as published by darkreading.com on October 4, 2012.



Copyright © SPAMfighter 2003-2012

<http://www.spamfighter.com/News-17993-Saliently-Sality-Botnet-Trapped-Scanning-IPv4-Address-Space.htm>

Module Objectives

CEH
Certified Ethical Hacker

- ☐ Overview of Network Scanning
- ☐ CEH Scanning Methodology
- ☐ Checking for Live Systems
- ☐ Scanning Techniques
- ☐ IDS Evasion Techniques
- ☐ Banner Grabbing
- ☐ Vulnerability Scanning
- ☐ Drawing Network Diagrams

- ☐ Use of Proxies for Attack
- ☐ Proxy Chaining
- ☐ HTTP Tunneling Techniques
- ☐ SSH Tunneling
- ☐ Anonymizers
- ☐ IP Spoofing Detection Techniques
- ☐ Scanning Countermeasures
- ☐ Scanning Pen Testing



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



Module Objectives

Once an attacker identifies his/her target system and does the initial reconnaissance, as discussed in the footprinting and reconnaissance module, the attacker concentrates on getting a **mode of entry** into the **target system**. It should be noted that scanning is not limited to intrusion alone. It can be an extended form of reconnaissance where the attacker learns more about his/her target, such as what operating system is used, the services that are being run on the systems, and **configuration lapses** if any can be identified. The **attacker** can then strategize his/her attack, factoring in these aspects.

This module will familiarize you with:

- | | |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none">☛ Overview of Network Scanning☛ CEH Scanning Methodology☛ Checking for Live Systems☛ Scanning Techniques☛ IDS Evasion Techniques☛ Banner Grabbing☛ Vulnerability Scanning☛ Drawing Network Diagrams | <ul style="list-style-type: none">☛ Use of Proxies for Attack☛ Proxy Chaining☛ HTTP Tunneling Techniques☛ SSH Tunneling☛ Anonymizers☛ IP Spoofing Detection Techniques☛ Scanning Countermeasures☛ Scanning Pen Testing |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Overview of Network Scanning

C|EH
Certified Ethical Hacker

- Network scanning refers to a set of procedures for identifying hosts, ports, and services in a network
- Network scanning is one of the components of intelligence gathering an attacker uses to create a profile of the target organization

The diagram illustrates the process of network scanning. On the left, labeled 'Attacker', there is a person wearing a mask and a hoodie, sitting at a desk with a computer monitor. A blue dashed arrow labeled 'Sends TCP /IP probes' points from the attacker to a group of three computer monitors on the right, labeled 'Network'. A blue dashed arrow labeled 'Gets network information' points from the network back to the attacker.

Objectives of Network Scanning

- To discover live hosts, IP address, and open ports of live hosts
- To discover operating systems and system architecture
- To discover services running on hosts
- To discover vulnerabilities in live hosts

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



Overview of Network Scanning

As we already discussed, **footprinting** is the first phase of hacking in which the attacker gains information about a potential target. Footprinting alone is not enough for hacking because here you will gather only the primary information about the target. You can use this primary information in the next phase to gather many more details about the target. The process of **gathering additional details** about the target using highly complex and aggressive reconnaissance techniques is called **scanning**.

The idea is to discover **exploitable communication channels**, to probe as many listeners as possible, and to keep track of the ones that are responsive or useful for hacking. In the scanning phase, you can find various ways of intruding into the target system. You can also discover more about the **target system**, such as what **operating system** is used, what **services** are **running**, and whether or not there are any **configuration lapses** in the target system. Based on the facts that you gather, you can form a strategy to launch an attack.

Types of Scanning

- Port scanning - Open ports and services
- Network scanning - IP addresses
- Vulnerability scanning - Presence of known weaknesses

In a traditional sense, the **access points** that a thief looks for are the doors and windows. These are usually the house's points of vulnerability because of their relatively easy accessibility. When it comes to computer systems and networks, **ports** are the doors and windows of the system that an intruder uses to gain access. The more the ports are open, the more points of vulnerability, and the fewer the ports open, the more secure the system is. This is simply a general rule. In some cases, the level of vulnerability may be high even though few ports are open.

Network scanning is one of the most important phases of intelligence gathering. During the network scanning process, you can gather information about specific IP addresses that can be accessed over the Internet, their targets' operating systems, system architecture, and the services running on each computer. In addition, the attacker also gathers details about the networks and their individual host systems.

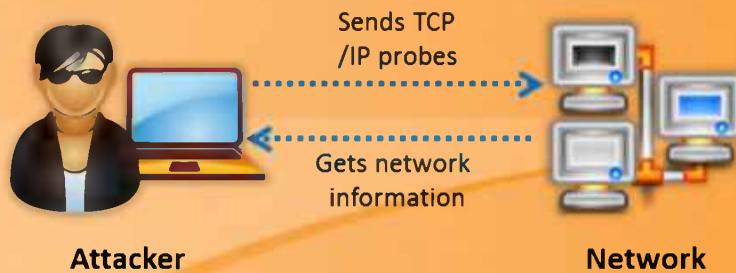


FIGURE 3.1: Network Scanning Diagram



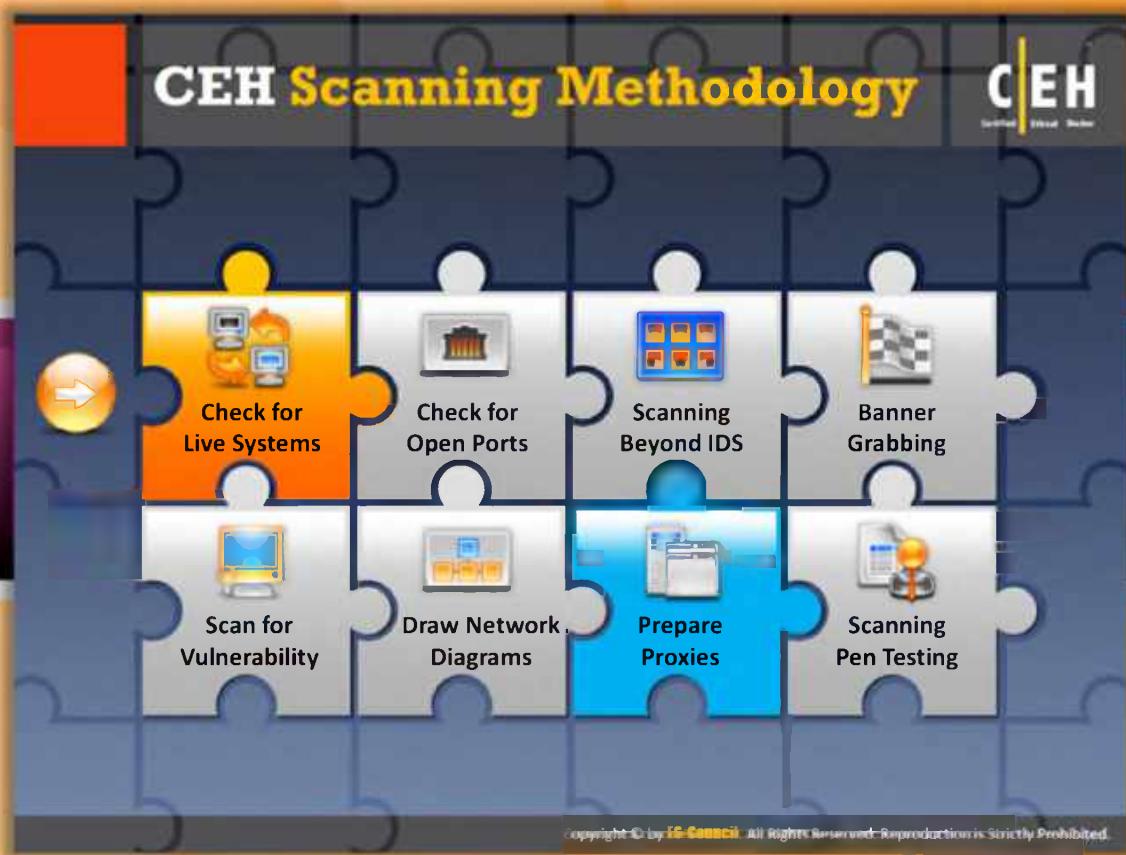
Objectives of Network Scanning

If you have a large amount of information about a **target organization**, there are greater chances for you to learn the **weakness** and **loopholes** of that particular organization, and consequently, for gaining unauthorized access to their network.

Before launching the attack, the attacker observes and analyzes the target network from different perspectives by performing different types of **reconnaissance**. How to perform scanning and what type of information to be achieved during the scanning process entirely depends on the hacker's viewpoint. There may be many objectives for performing scanning, but here we will discuss the most common objectives that are encountered during the hacking phase:

- ➊ **Discovering live hosts, IP address, and open ports of live hosts running on the network.**
- ➋ **Discovering open ports:** Open ports are the best means to break into a system or network. You can find easy ways to break into the target organization's network by discovering open ports on its network.
- ➌ **Discovering operating systems and system architecture of the targeted system:** This is also referred to as fingerprinting. Here the attacker will try to launch the attack based on the operating system's vulnerabilities.

- ② **Identifying the vulnerabilities and threats:** Vulnerabilities and threats are the **security risks** present in any system. You can compromise the system or network by exploiting these vulnerabilities and threats.
- ③ **Detecting the associated network service of each port**



CEH Scanning Methodology

The first step in scanning the network is to **check for live systems**.

 Check for Live Systems	 Scan for Vulnerability
 Check for Open Ports	 Draw Network Diagrams
 Scanning Beyond IDS	 Prepare Proxies
 Banner Grabbing	 Scanning Pen Testing

This section highlights how to check for live systems with the help of ICMP scanning, how to ping a system and various ping sweep tools.

Checking for Live Systems - ICMP Scanning

C|EH Certified Ethical Hacker

- Ping scan involves sending **ICMP ECHO requests** to a host. If the host is live, it will return an ICMP ECHO reply
- This scan is useful for **locating active devices** or determining if **ICMP is passing through a firewall**

The ping scan output using Nmap:

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



Checking for Live Systems - ICMP Scanning

ICMP Scanning

All required information about a system can be gathered by **sending ICMP packets** to it. Since ICMP does not have a port abstraction, this cannot be considered a case of port scanning. However, it is useful to determine which hosts in a network are up by pinging them all (the **-P** option does this; ICMP scanning is now in parallel, so it can be quick). The user can also increase the number of pings in parallel with the **-L** option. It can also be helpful to tweak the ping timeout value with the **-T** option.

ICMP Query

The UNIX tool **ICMPquery** or **ICMPPush** can be used to request the time on the system (to find out which time zone the system is in) by sending an ICMP type 13 message (TIMESTAMP). The netmask on a particular system can also be determined with ICMP type 17 messages (ADDRESS MARK REQUEST). After finding the netmask of a network card, one can determine all the subnets in use. After gaining information about the subnets, one can target only one particular subnet and avoid hitting the broadcast addresses.

ICMPquery has both a timestamp and address mask request option:

```
icmp query <-query-> [-B] [-f fromhost] [-d delay] [-T time] target
```

Where

<query> is one of:

- t: icmp timestamp request (default)
- m: icmp address mask request
- d: delay to sleep between packets is in microseconds.

-T - specifies the number of seconds to wait for a host to respond. The default is 5.

A target is a list of hostnames or addresses.



FIGURE 3.2: ICMP Query Diagram

Ping Scan Output Using Nmap

Source: <http://nmap.org>

Nmap is a tool that can be used for ping scans, also known as host discovery. Using this tool you can determine the live hosts on a network. It performs ping scans by sending the ICMP ECHO requests to all the hosts on the network. If the host is live, then the host sends an ICMP ECHO reply. This scan is useful for locating active devices or determining if ICMP is passing through a firewall.

The following screenshot shows the sample output of a ping scan using **Zenmap**, the official cross-platform GUI for the Nmap Security Scanner:

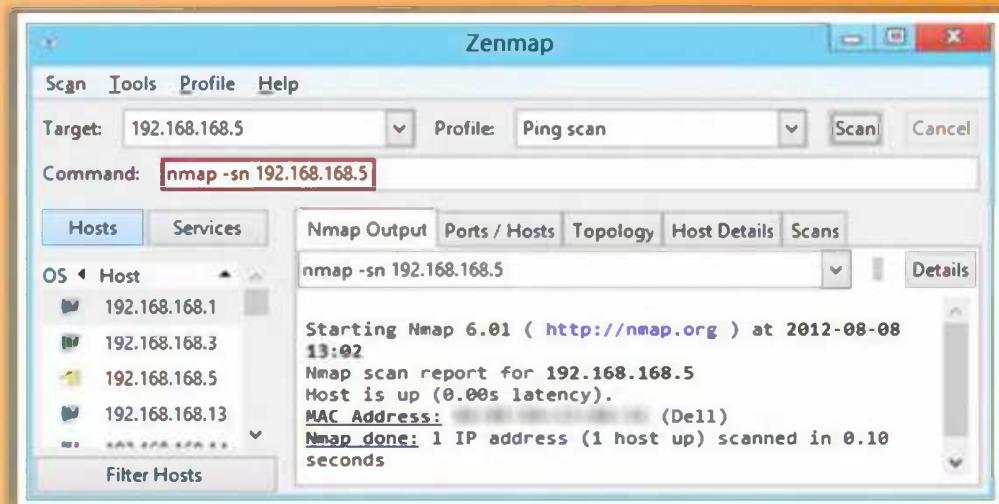


FIGURE 3.3: Zenmap Showing Ping Scan Output

Ping Sweep

C|EH Certified Ethical Hacker

- Ping sweep is used to determine the **live hosts from a range of IP addresses** by sending ICMP ECHO requests to multiple hosts. If a host is live, it will return an ICMP ECHO reply
- Attackers calculate subnet masks using **Subnet Mask Calculators** to identify the number of hosts present in the subnet
- Attackers then use ping sweep to create an **inventory of live systems** in the subnet

The ping sweep output using Nmap

Zenmap

Targets: 192.168.1.0-50

Command: nmap -sn -PE PA21,23,80,192.168.1.50

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

OS: Host 192.168.1.1 Host 192.168.1.3 Host 192.168.1.13 Host 192.168.1.14 Host 192.168.1.15 Host 192.168.1.17 Host 192.168.1.19 Host 192.168.1.28 Host 192.168.1.29

Starting Nmap 6.01 (http://nmap.org) at 2013-08-08 12:41 EDT

Hosts up (0.08s latency).

Nmap scan report for 192.168.1.1

Host is up (0.08s latency).

MAC Address: 00:0C:29 (Hewlett-Packard Company)

Nmap scan report for 192.168.1.3

Host is up (0.08s latency).

MAC Address: 00:0C:29 (Hewlett-Packard Company)

Nmap scan report for 192.168.1.13

Host is up (0.08s latency).

MAC Address: 00:0C:29 (Apple)

Nmap scan report for 192.168.1.14

Host is up (0.08s latency).

MAC Address: 00:0C:29 (Apple)

Nmap scan report for 192.168.1.15

Host is up (0.08s latency).

MAC Address: 00:0C:29 (Apple)

Nmap scan report for 192.168.1.17

Host is up (0.08s latency).

MAC Address: 00:0C:29 (Dell)

Nmap scan report for 192.168.1.19

Host is up (0.08s latency).

MAC Address: 00:0C:29 (Dell)

Nmap scan report for 192.168.1.28

Host is up (0.08s latency).

MAC Address: 00:0C:29 (Foxconn)

Nmap scan report for 192.168.1.29

Host is up (0.08s latency).

MAC Address: 00:0C:29 (Foxconn)

http://nmap.org

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



A ping sweep (also known as an **ICMP sweep**) is a basic network scanning technique to determine which range of IP addresses map to **live hosts** (computers). While a single ping tells the user whether one specified host computer exists on the network, a ping sweep consists of ICMP ECHO requests sent to multiple hosts.

ICMP ECHO Reply

If a host is active, it returns an **ICMP ECHO** reply. Ping sweeps are among the oldest and slowest methods to scan a network. This utility is distributed across almost all platforms, and acts like a roll call for systems; a system that is live on the network answers the ping query that is sent by another system.

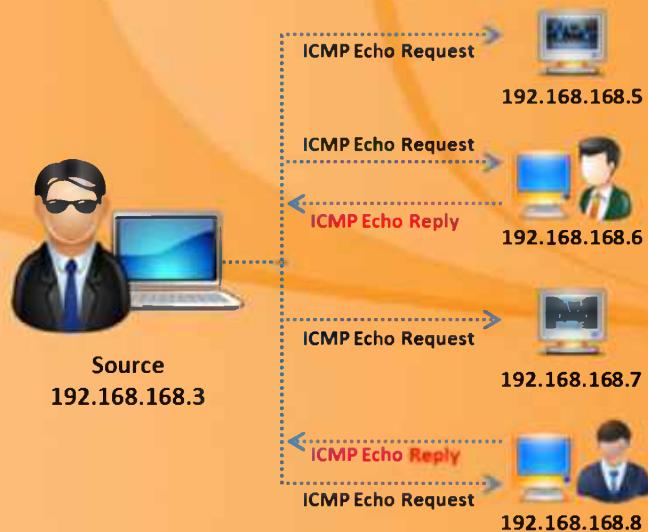


FIGURE 3.4: Ping Sweep Diagram

TCP/IP Packet

To understand ping, you should be able to understand the **TCP/IP packet**. When a system pings, a single packet is sent across the network to a specific IP address. This packet contains **64 bytes**, i.e., **56 data bytes** and **8 bytes** of protocol header information. The sender then waits for a return packet from the target system. A good return packet is expected only when the connections are good and when the targeted system is active. Ping also determines the number of hops that lie between the two computers and the **round-trip time**, i.e., the total time taken by a packet for completing a trip. Ping can also be used for resolving host names. In this case, if the packet bounces back when sent to the IP address, but not when sent to the name, then it is an indication that the system is unable to resolve the name to the specific IP address.

Source: <http://nmap.org>

Using **Nmap Security Scanner** you can perform ping sweep. Ping sweep determines the IP addresses of live hosts. This provides information about the live host IP addresses as well as their MAC address. It allows you to scan multiple hosts at a time and determine active hosts on the network. The following screenshot shows the result of a ping sweep using Zenmap, the official cross-platform GUI for the Nmap Security Scanner:

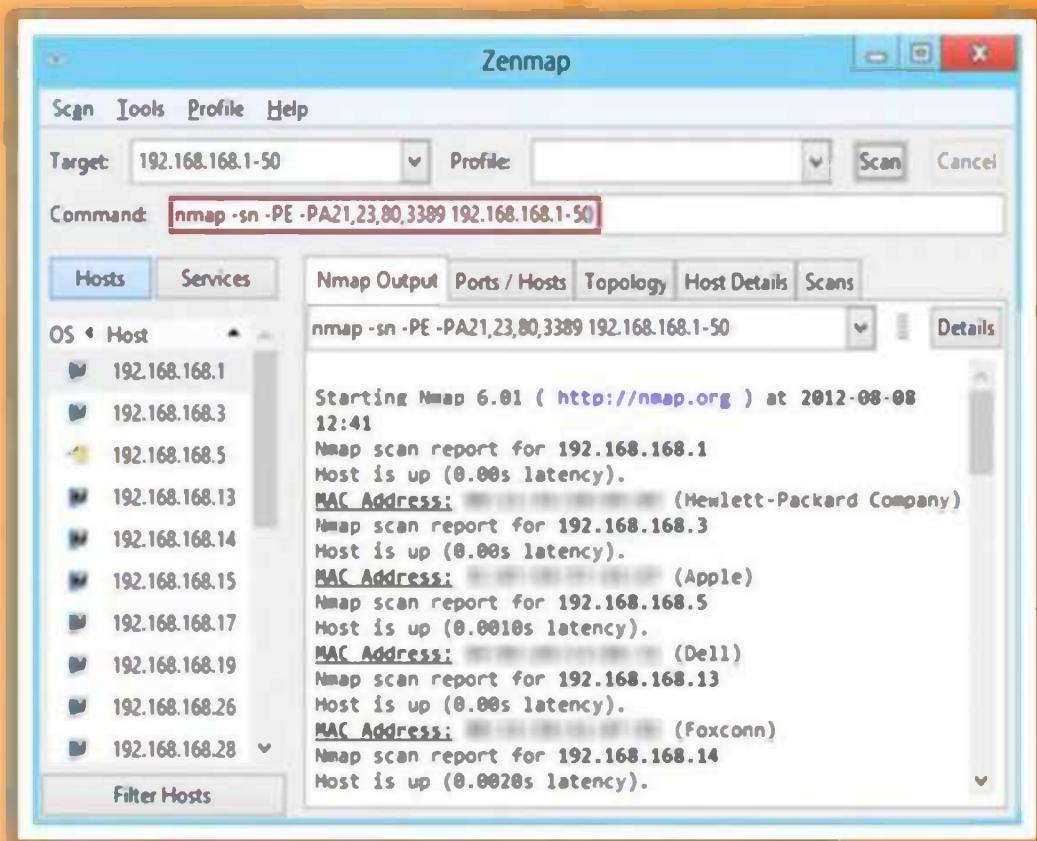
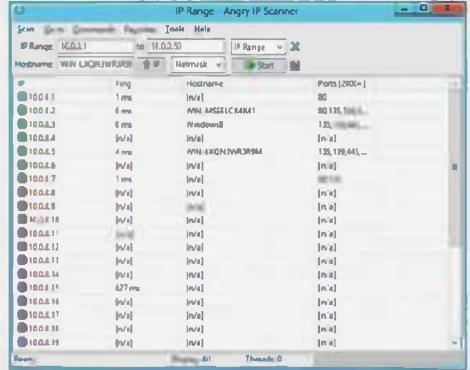


FIGURE 3.5: Zenmap showing ping sweep output

Ping Sweep Tools

Angry IP Scanner pings each IP address to check if it's alive, then optionally resolves its hostname, determines the MAC address, scans ports, etc.



SolarWinds Engineer Toolset's Ping Sweep enables scanning a range of IP addresses to identify which IP addresses are in use and which ones are currently free. It also performs reverse DNS lookup.



<http://www.angryip.org>

<http://www.solarwinds.com>

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

Ping Sweep Tools

Determining live hosts on a target network is the first step in the process of **hacking or breaking** into a network. This can be done using ping sweep tools. There are a number of ping sweep tools readily available in the market using which you can perform ping sweeps easily. These tools allow you to determine the live hosts by sending ICMP ECHO requests to multiple hosts at a time. **Angry IP Scanner** and **Solarwinds Engineer's Toolset** are a few commonly used ping sweep tools.



Angry IP Scanner

Source: <http://www.angryip.org>

Angry IP Scanner is an **IP scanner tool**. This tool identifies all non-responsive addresses as dead nodes, and resolves hostname details, and checks for open ports. The main feature of this tool is multiple ports scanning, configuring scanning columns. Its main goal is to find the active hosts in the network by scanning all the IP addresses as well as ports. It runs on Linux, Windows, Mac OS X, etc. It can scan IP addresses ranging from **1.1.1.1** to **255.255.255.255**.

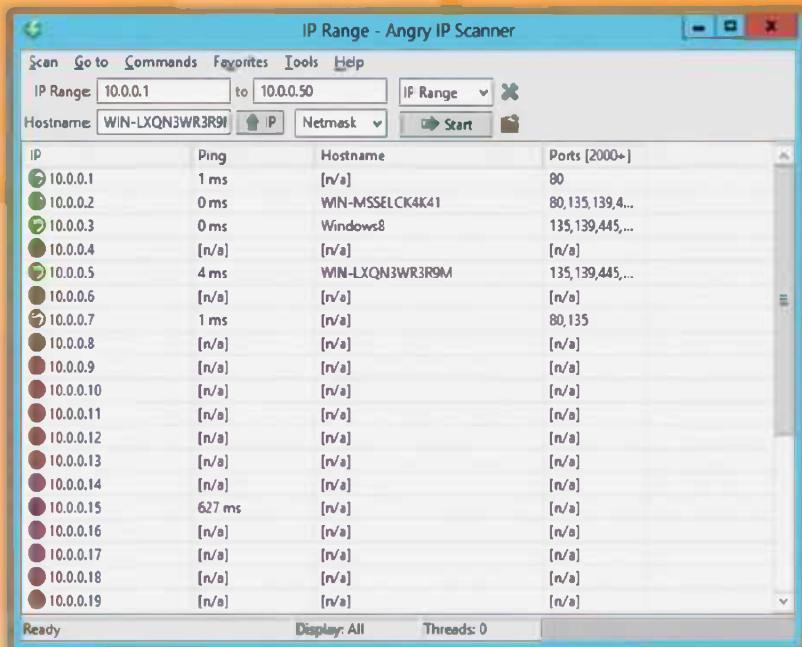


FIGURE 3.6: Angry IP Scanner Screenshot



Solarwinds Engineer's Toolset

Source: <http://www.solarwinds.com>

The Solarwinds Engineer's Toolset is a collection of **network engineer's tools**. By using this toolset you can scan a range of IP addresses and can identify the IP addresses that are in use currently and the IP addresses that are free. It also performs **reverse DNS lookup**.

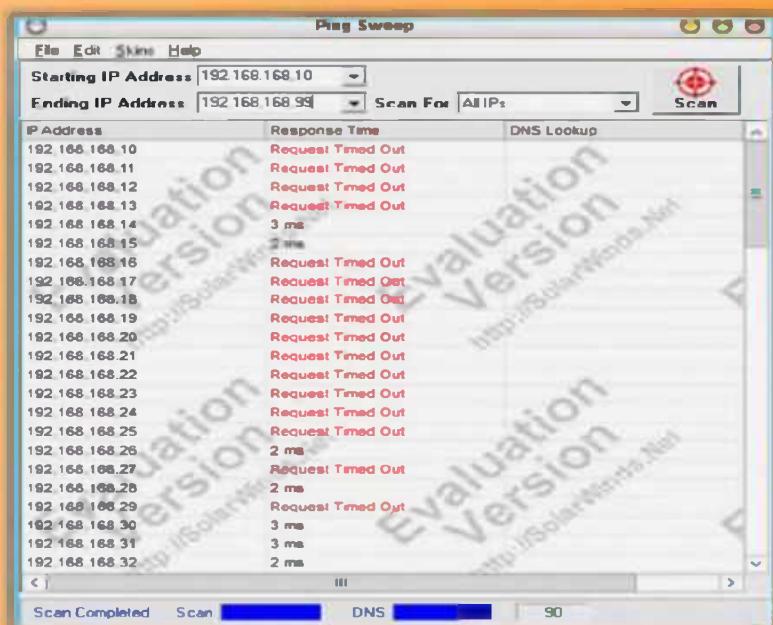


FIGURE 3.7: Solarwinds Engineer's Toolset Screenshot

Ping Sweep Tools (Cont'd)



 Colasoft Ping Tool http://www.colasoft.com	 PacketTrap MSP http://www.packettrap.com
 Visual Ping Tester - Standard http://www.pingtester.net	 Ping Sweep http://www.whatsupgold.com
 Ping Scanner Pro http://www.digilextechnologies.com	 Network Ping http://www.greenline-soft.com
 Ultra Ping Pro http://ultraping.webs.com	 Ping Monitor http://www.niliand.com
 PingInfoView http://www.nirsoft.net	 Pinkie http://www.ipuptime.net

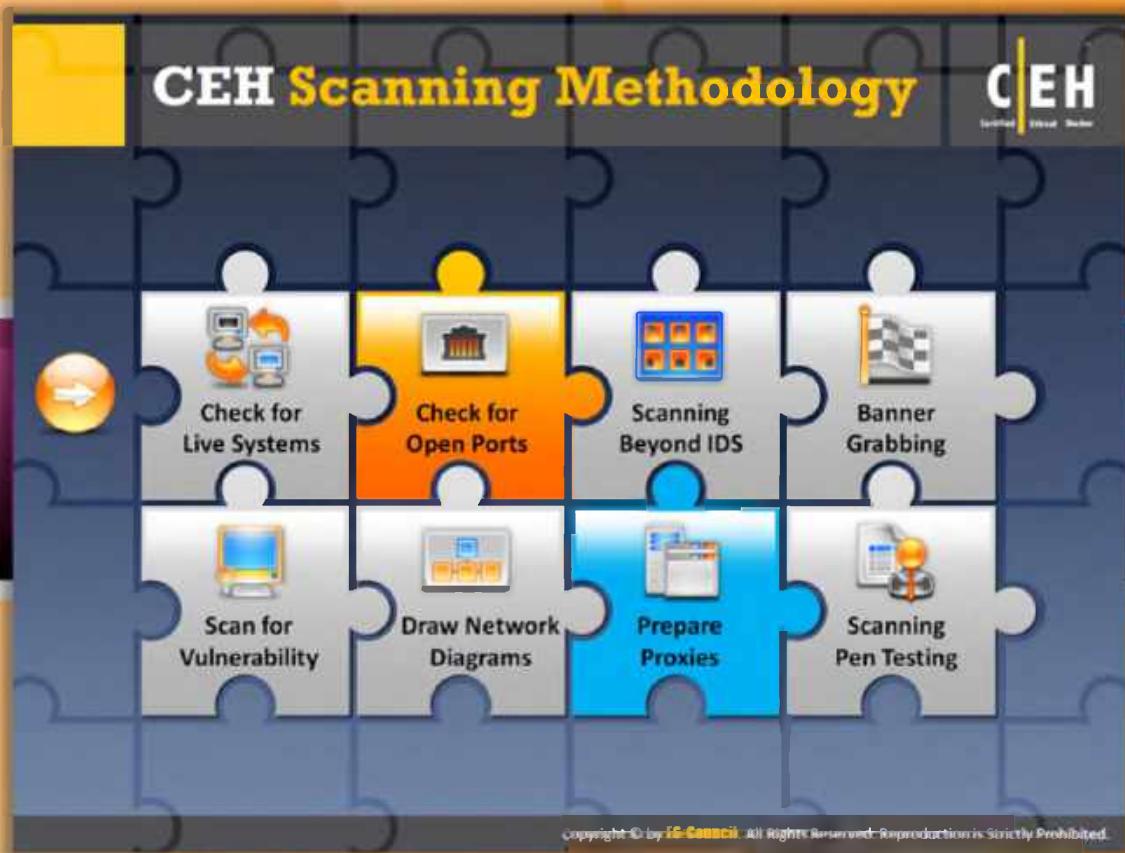
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



Ping Sweep Tools (Cont'd)

In addition to Solarwinds Engineer's Toolset and Angry IP Scanner, there are many other tools that feature ping sweep capabilities. For example:

- ⌚ Colasoft Ping Tool available at <http://www.colasoft.com>
- ⌚ Visual Ping Tester – Standarad available at <http://www.pingtester.net>
- ⌚ Ping Scanner Pro available at <http://www.digilextechnologies.com>
- ⌚ Ultra Ping Pro available at <http://ultraping.webs.com>
- ⌚ PingInfoView available at <http://www.nirsoft.net>
- ⌚ PacketTrap MSP available at <http://www.packettrap.com>
- ⌚ Ping Sweep available at <http://www.whatsupgold.com>
- ⌚ Network Ping available at <http://www.greenline-soft.com>
- ⌚ Ping Monitor available at <http://www.niliand.com>
- ⌚ Pinkie available at <http://www.ipuptime.net>



CEH Scanning Methodology

So far we discussed how to check for live systems. Open ports are the doorways for an attacker to launch attacks on systems. Now we will discuss scanning for open ports.

 Check for Live Systems	 Scan for Vulnerability
 Check for Open Ports	 Draw Network Diagrams
 Scanning Beyond IDS	 Prepare Proxies
 Banner Grabbing	 Scanning Pen Testing

This section covers the three-way handshake, scanning IPv6 networks, and various scanning techniques such as FIN scan, SYN scan, and so on.

Three-Way Handshake

C|EH Certified Ethical Hacker

TCP uses a **three-way handshake** to establish a connection between server and client

Three-way Handshake Process

1. The Computer A (10.0.0.2) initiates a connection to the server (10.0.0.3) via a packet with only the **SYN** flag set
2. The server replies with a packet with both the **SYN** and the **ACK** flag set
3. For the final step, the client responds back to the server with a single **ACK** packet
4. If these three steps are completed without complication, then a TCP connection is established between the client and the server

Step 1
Step 2
Step 3

Client: Bill (10.0.0.2:21)

Server: Sheela (10.0.0.3:21)

Sequence:

- Step 1: Bill → Sheela: SYN, SEQ# 10
- Step 2: Sheela → Bill: SYN + ACK, ACK# 11, SEQ# 11
- Step 3: Bill → Sheela: ACK, ACK# 11, SEQ# 11

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



Three-Way Handshake

TCP is connection-oriented, which implies connection establishment is principal prior to data transfer between applications. This connection is possible through the process of the three-way handshake. The three-way handshake is implemented for establishing the **connection between protocols**.

The **three-way handshake process goes as follows:**

- >To launch a **TCP connection**, the source (10.0.0.2:62000) sends a SYN packet to the destination (10.0.0.3:21).
- The destination, on receiving the SYN packet, i.e., sent by the source, responds by sending a SYN/ACK packet back to the source.
- This ACK packet confirms the arrival of the first SYN packet to the source.
- In conclusion, the source sends an ACK packet for the ACK/SYN packet sent by the destination.
- This triggers an "**OPEN**" connection allowing communication between the source and the destination, until either of them issues a "FIN" packet or a "RST" packet to close the connection.

The TCP protocol maintains stateful connections for all connection-oriented protocols across the Internet, and works the same as an ordinary telephone communication, in which one picks up a telephone receiver, hears a dial tone, and dials a number that triggers ringing at the other end until a person picks up the receiver and says, "Hello."

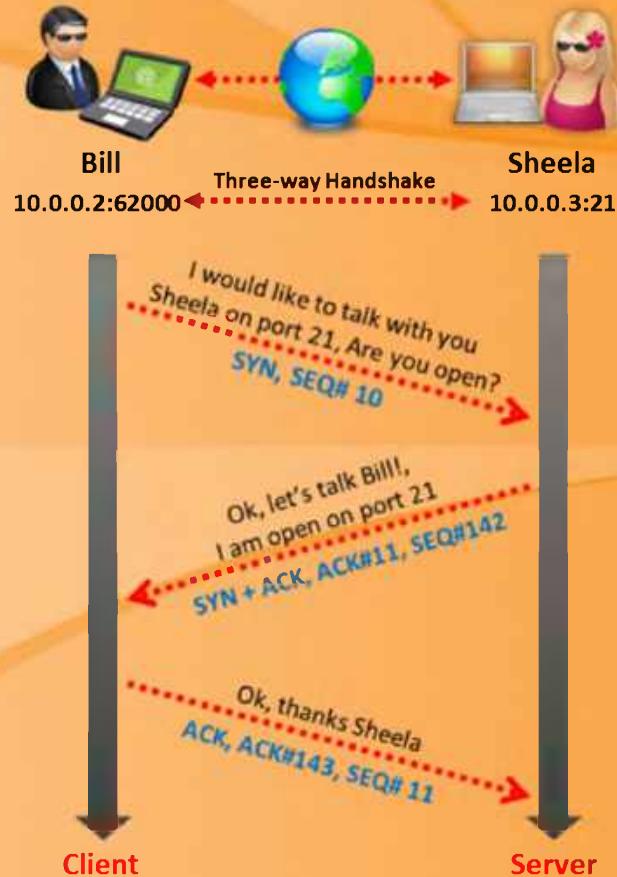


FIGURE 3.8: Three-way Handshake Process



Establishing a TCP Connection

As we previously discussed, a TCP connection is established based on the three-way hand shake method. It is clear from the name of the connection method that the establishment of the connection is accomplished in **three main steps**.

Source: <http://support.microsoft.com/kb/172983>

The following three frames will explain the establishment of a TCP connection between nodes NTW3 and BDC3:

Frame 1:

In the first step, the client, NTW3, sends a SYN segment (TCPS.). This is a request to the server to synchronize the sequence numbers. It specifies its Initial Sequence Number (ISN), which is incremented by 1 and that is sent to the server. To initialize a connection, the client and server must synchronize each other's sequence numbers. There is also an option for the

Maximum Segment Size (MSS) to be set, which is defined by the length (len: 4), this option communicates the maximum segment size the sender wants to receive. The Acknowledgement field (ack: 0) is set to zero because this is the first part of the three-way handshake.

```
1    2.0785 NTW3 --> BDC3 TCP ....S., len: 4, seq: 8221822-8221825, ack: 0,  
win: 8192, src: 1037 dst: 139 (NBT Session) NTW3 --> BDC3 IP  
TCP: ....S., len: 4, seq: 8221822-8221825, ack: 0, win: 8192, src: 1037  
dst: 139 (NBT Session)
```

```
TCP: Source Port = 0x040D  
TCP: Destination Port = NETBIOS Session Service  
TCP: Sequence Number = 8221822 (0x7D747E)  
TCP: Acknowledgement Number = 0 (0x0)  
TCP: Data Offset = 24 (0x18)  
TCP: Reserved = 0 (0x0000)  
TCP: Flags = 0x02 : ....S.
```

```
TCP: ..0..... = No urgent data  
TCP: ...0..... = Acknowledgement field not significant  
TCP: ....0... = No Push function  
TCP: .....0.. = No Reset  
TCP: .....1. = Synchronize sequence numbers  
TCP: .....0 = No Fin
```

```
TCP: Window = 8192 (0x2000)  
TCP: Checksum = 0xF213  
TCP: Urgent Pointer = 0 (0x0)  
TCP: Options
```

```
TCP: Option Kind (Maximum Segment Size) = 2 (0x2)  
TCP: Option Length = 4 (0x4)  
TCP: Option Value = 1460 (0x5B4)  
TCP: Frame Padding
```

```
00000: 02 60 8C 9E 18 8B 02 60 8C 3B 85 C1 08 00 45 00 .`.....`.;....E.  
00010: 00 2C 0D 01 40 00 80 06 E1 4B 83 6B 02 D6 83 6B .,...@....K.k...k  
00020: 02 D3 04 0D 00 8B 00 7D 74 7E 00 00 00 00 60 02 .....}t~....`.  
00030: 20 00 F2 13 00 00 02 04 05 B4 20 20 .....
```

Frame 2:

In the second step, the server, BDC3, sends an ACK and a SYN on this segment (TCP .A..S.). In this segment the server is acknowledging the request of the client for synchronization. At the same time, the server is also sending its request to the client for synchronization of its sequence numbers. There is one major difference in this segment. The server transmits an acknowledgement number (8221823) to the client. The acknowledgement is just proof to the client that the ACK is specific to the SYN the client initiated. The process of acknowledging the client's request allows the server to increment the client's sequence number by one and uses it as its acknowledgement number.

```
2 2.0786 BDC3 --> NTW3  TCP .A..S., len: 4, seq: 1109645-1109648, ack:  
8221823, win: 8760, src: 139 (NBT Session) dst: 1037 BDC3 --> NTW3  IP  
TCP: .A..S., len: 4, seq: 1109645-1109648, ack: 8221823, win: 8760,  
src: 139 (NBT Session) dst: 1037  
TCP: Source Port = NETBIOS Session Service  
TCP: Destination Port = 0x040D  
TCP: Sequence Number = 1109645 (0x10EE8D)  
TCP: Acknowledgement Number = 8221823 (0x7D747F)  
TCP: Data Offset = 24 (0x18)  
TCP: Reserved = 0 (0x0000)  
TCP: Flags = 0x12 : .A..S.  
TCP: ..0..... = No urgent data  
TCP: ...1.... = Acknowledgement field significant  
TCP: ....0... = No Push function  
TCP: .....0.. = No Reset  
TCP: .....1. = Synchronize sequence numbers  
TCP: .....0 = No Fin  
TCP: Window = 8760 (0x2238)  
TCP: Checksum = 0x012D  
TCP: Urgent Pointer = 0 (0x0)  
TCP: Options  
TCP: Option Kind (Maximum Segment Size) = 2 (0x2)  
TCP: Option Length = 4 (0x4)  
TCP: Option Value = 1460 (0x5B4)  
TCP: Frame Padding
```

```
00000: 02 60 8C 3B 85 C1 02 60 8C 9E 18 8B 08 00 45 00 . .,.... ....E.  
00010: 00 2C 5B 00 40 00 80 06 93 4C 83 6B 02 D3 83 6B .,[.@....L.k...k  
00020: 02 D6 00 8B 04 0D 00 10 EE 8D 00 7D 74 7F 60 12 .....}t`.
```

00030: 22 38 01 2D 00 00 02 04 05 B4 20 20 "8.-.....

Frame 3:

In the third step, the client sends an ACK on this segment (TCP .A....). In this segment, the client is acknowledging the request from the server for synchronization. The client uses the same algorithm the server implemented in providing an acknowledgement number. The client's acknowledgement of the server's request for synchronization completes the process of establishing a reliable connection, thus the three-way handshake.

3 2.787 NTW3 --> BDC3 TCP .A...., len: 0, seq: 8221823-8221823, ack:
1109646, win: 8760, src: 1037 dst: 139 (NBT Session) NTW3 --> BDC3 IP

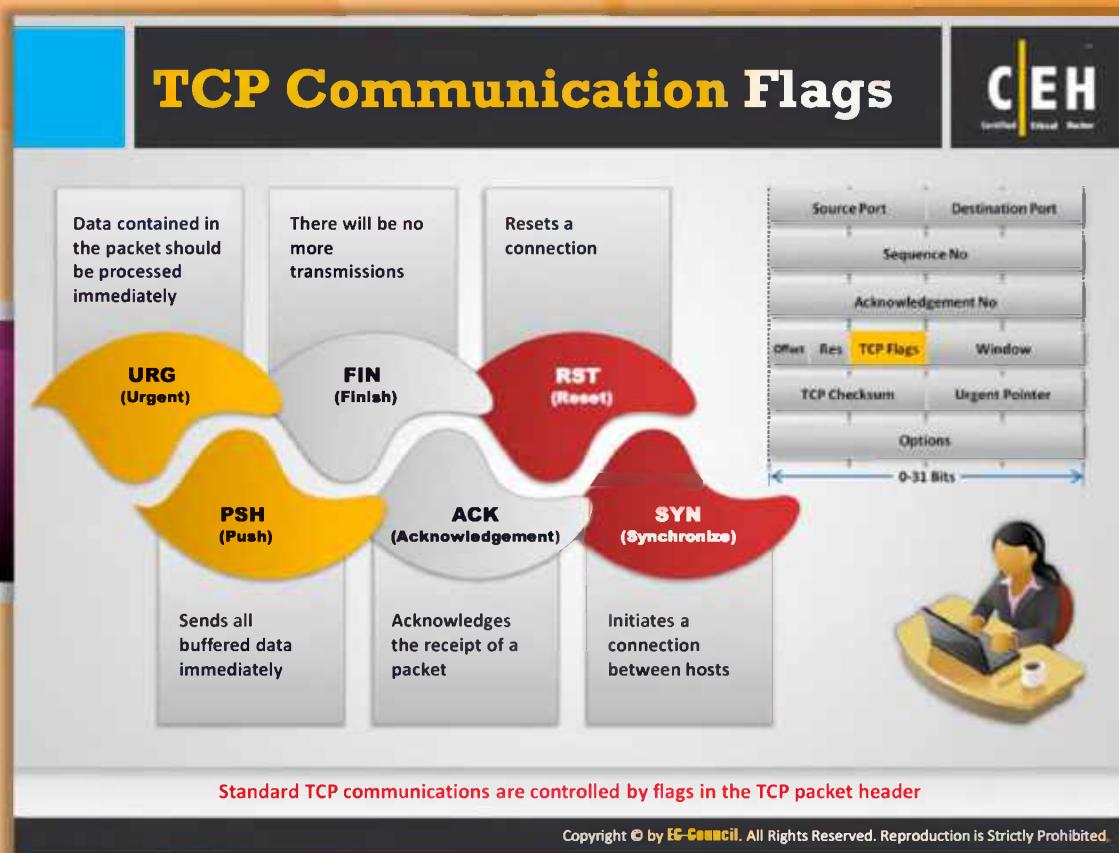
TCP: .A...., len: 0, seq: 8221823-8221823, ack: 1109646, win: 8760,
src: 1037 dst: 139 (NBT Session)

TCP: Source Port = 0x040D
TCP: Destination Port = NETBIOS Session Service
TCP: Sequence Number = 8221823 (0x7D747F)
TCP: Acknowledgement Number = 1109646 (0x10EE8E)
TCP: Data Offset = 20 (0x14)
TCP: Reserved = 0 (0x0000)
TCP: Flags = 0x10 : .A....

TCP: ..0..... = No urgent data
TCP: ...1.... = Acknowledgement field significant
TCP:0... = No Push function
TCP:0.. = No Reset
TCP:0. = No Synchronize
TCP:0 = No Fin

TCP: Window = 8760 (0x2238)
TCP: Checksum = 0x18EA
TCP: Urgent Pointer = 0 (0x0)
TCP: Frame Padding

00000: 02 60 8C 9E 18 8B 02 60 8C 3B 85 C1 08 00 45 00 .`.....`.;....E.
00010: 00 28 0E 01 40 00 80 06 E0 4F 83 6B 02 D6 83 6B .(..@....0.k...k
00020: 02 D3 04 0D 00 8B 00 7D 74 7F 00 10 EE 8E 50 10}t....P.
00030: 22 38 18 EA 00 00 20 20 20 20 20 20 20 20 20 "8....



TCP Communication Flags

Standard TCP communications monitor the **TCP packet header** that holds the flags. These flags govern the connection between hosts, and give instructions to the system. The following are the TCP communication flags:

- ⌚ Synchronize alias “**SYN**”: SYN notifies transmission of a new sequence number
- ⌚ Acknowledgement alias “**ACK**”: ACK confirms receipt of transmission, and identifies next expected sequence number
- ⌚ Push alias “**PSH**”: System accepting requests and forwarding buffered data
- ⌚ Urgent alias “**URG**”: Instructs data contained in packets to be processed as soon as possible
- ⌚ Finish alias “**FIN**”: Announces no more transmissions will be sent to remote system
- ⌚ Reset alias “**RST**”: Resets a connection

SYN scanning mainly deals with three of the flags, namely, SYN, ACK, and RST. You can use these three flags for gathering illegal information from servers during the enumeration process.

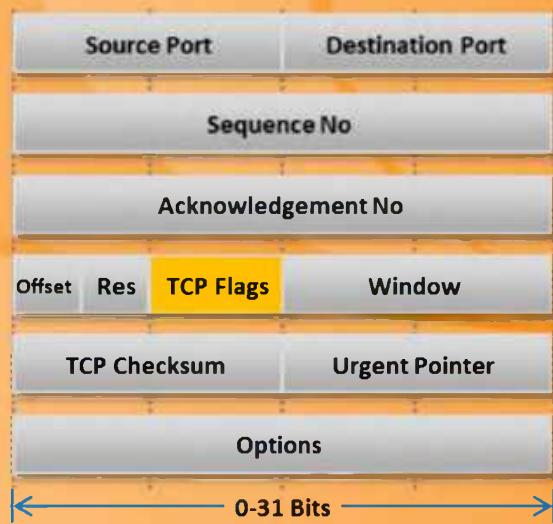
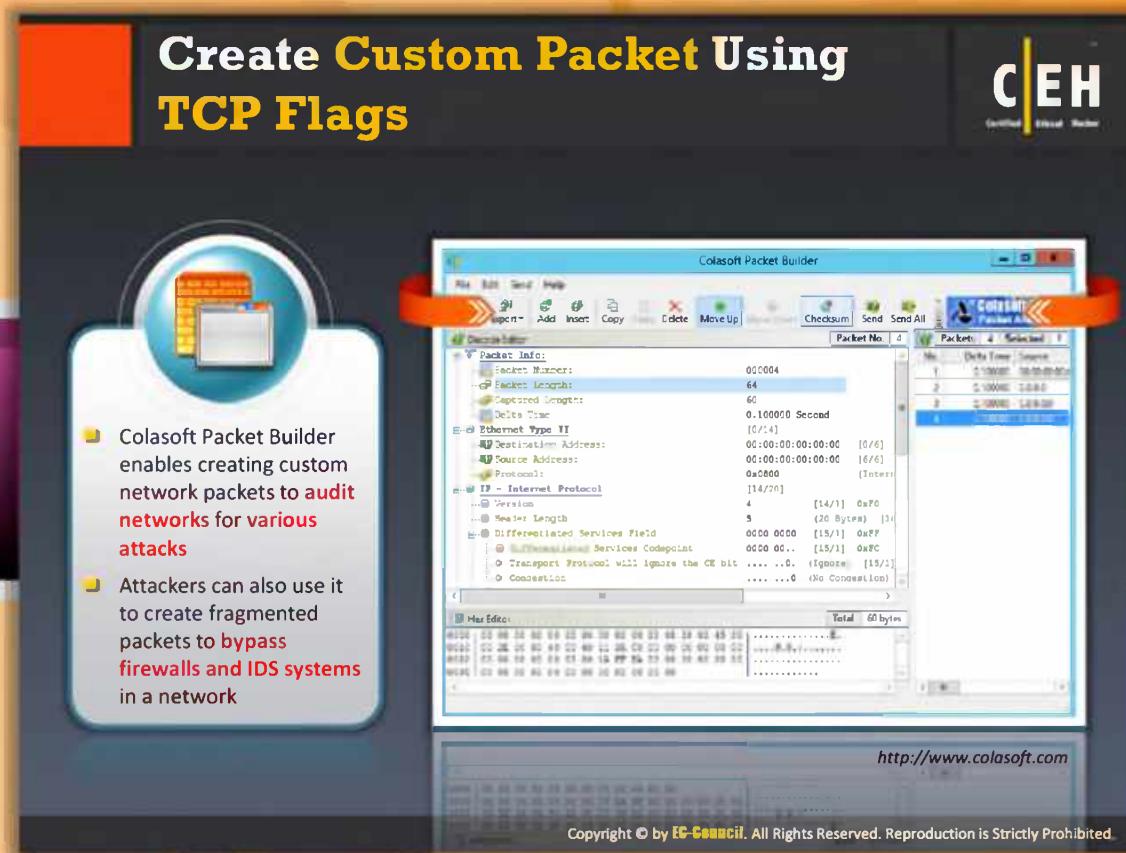


FIGURE 3.9: TCP Communication Flags



Create Custom Packets using TCP Flags

Source: <http://www.colasoft.com>

Colasoft Packet Builder is a tool that allows you to create **custom network packets** and also allows you to check the network against various attacks. It allows you to select a **TCP packet** from the provided templates, and **change the parameters** in the decoder editor, hexadecimal editor, or ASCII editor to create a packet. In addition to building packets, **Colasoft Packet Builder** also supports **saving** packets to packet files and **sending** packets to the network.

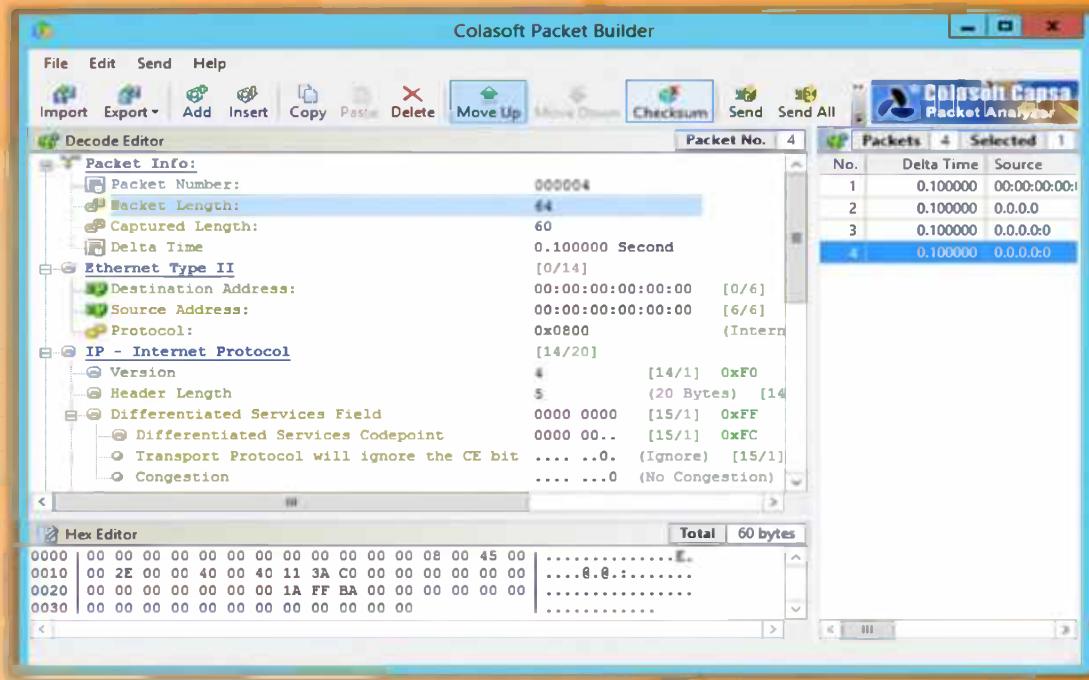


FIGURE 3.10: Colasoft Packet Builder Screenshot

Scanning IPv6 Network

C|EH
Certified Ethical Hacker

- IPv6 increases the IP address size from **32 bits to 128 bits**, to support more levels of addressing hierarchy
- Traditional network scanning techniques will be **computationally less feasible** due to larger search space (64 bits of host address space or 2^{64} addresses) provided by IPv6 in a subnet
- Scanning in IPv6 network is more difficult and complex than the IPv4 and also major scanning tools such as **Nmap** do not support ping sweeps on **IPv6 networks**
- Attackers need to harvest IPv6 addresses from **network traffic**, **recorded logs** or **Received from:** and other header lines in archived email or Usenet news messages
- Scanning IPv6 network, however, offers a large number of hosts in a subnet if an attacker can compromise one host in the subnet; attacker can probe the "**all hosts**" link local multicast address

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



Scanning IPv6 Network

IPv6 increases the size of **IP address space** from **32 bits to 128 bits** to support more levels of addressing hierarchy. Traditional network scanning techniques will be computationally less feasible due to **larger search space** (64 bits of host address space or 2^{64} addresses) provided by IPv6 in a subnet. Scanning an IPv6 network is more difficult and complex than IPv4 and also major scanning tools such as Nmap **do not support ping sweeps on IPv6 networks**. Attackers need to harvest IPv6 addresses from network traffic, recorded logs, or Received from: and other header lines in archived email or Usenet news messages to identify IPv6 addresses for subsequent port scanning. Scanning IPv6 network, however, offers **a large number of hosts in a subnet**; if an attacker can compromise one host in the subnet he can probe the "all hosts" link local multicast address.

Scanning Tool: Nmap

C|EH
Certified Ethical Hacker

- Network administrators can use Nmap for **network inventory**, managing service upgrade schedules, and **monitoring host or service uptime**
- Attacker uses Nmap to extract information such as **live hosts on the network**, **services** (application name and version), type of **packet filters/firewalls**, **operating systems** and **OS versions**

The image shows two windows of the Nmap command-line interface. The left window displays a detailed list of open ports and services for a target host, including port numbers, protocols, and service names like 'Apache'. The right window shows a similar list for another host, with some ports being 'closed' and others 'filtered'. Both windows have a standard Windows-style interface with tabs for 'Ports', 'Services', and 'Script'. The URL <http://nmap.org> is visible at the bottom right of the slide.

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



Scanning Tool: Nmap

Source: <http://nmap.org>

Nmap is a **security scanner** for network exploration and hacking. It allows you to discover hosts and services on a computer network, thus creating a "map" of the network. It sends specially **crafted packets** to the target host and then analyzes the responses to accomplish its goal. Either a network administrator or an attacker can use this tool for their particular needs. Network administrators can use Nmap for **network inventory**, **managing service upgrade** schedules, and **monitoring host** or service uptime. Attackers use Nmap to extract information such as live hosts on the network, services (application name and version), type of packet filters/firewalls, **operating systems**, and **OS versions**.

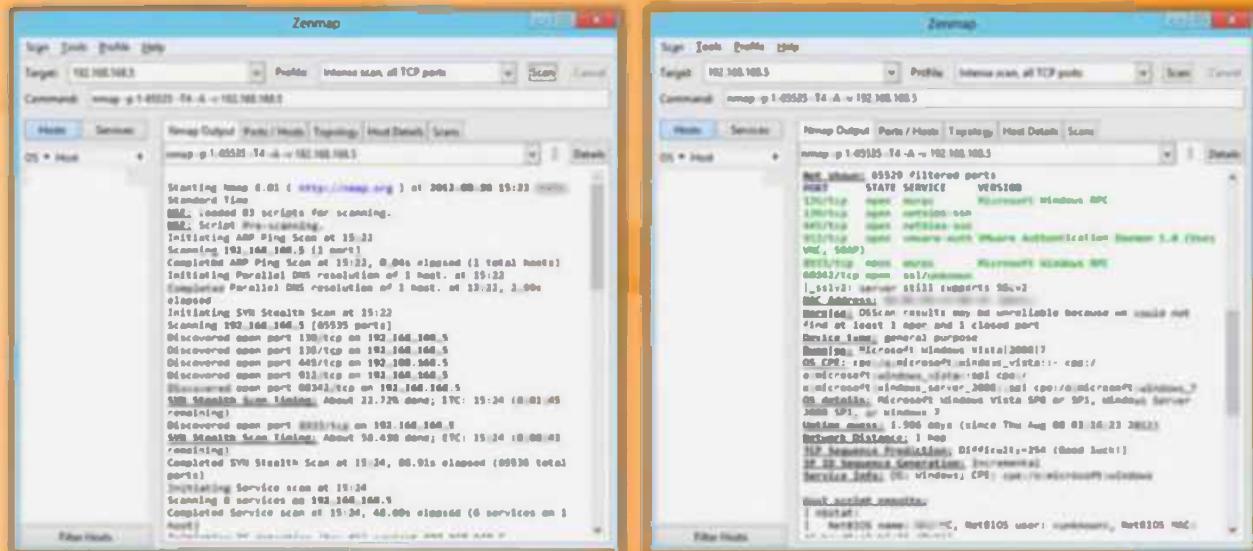


FIGURE 3.11: Zenmap Screenshots

Hping2 / Hping3

CEH
Certified Ethical Hacker

- Command line **packet crafter** for the TCP/IP protocol
- Tool for **security auditing** and **testing firewall and networks**
- Runs on both **Windows** and **Linux operating systems**

<http://www.hping.org>

ICMP Scanning

ACK Scanning on port 80

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



Hping2/Hping3

Source: <http://www.hping.org>

HPing2/HPing3 is a **command-line-oriented TCP/IP** packet assembler/analyzer that sends ICMP echo requests and supports TCP, UDP, ICMP, and raw-IP protocols. It has **Traceroute mode**, and enables you to send files between covert channels. It has the ability to send custom TCP/IP packets and display target replies like a ping program does with **ICMP replies**. It handles fragmentation, arbitrary packets' body and size, and can be used in order to transfer encapsulated files under supported protocols. It supports idle host scanning. IP spoofing and **network/host** scanning can be used to perform an anonymous probe for services.

An attacker studies the behavior of an idle host to gain information about the target such as the services that the host offers, the ports supporting the services, and the operating system of the target. This type of scan is a predecessor to either heavier probing or outright attacks.

Features:

The following are some of the features of HPing2/HPing3:

- Determines whether the host is up even when the host blocks ICMP packets
- Advanced port scanning** and test net performance using different protocols, packet sizes, TOS, and fragmentation

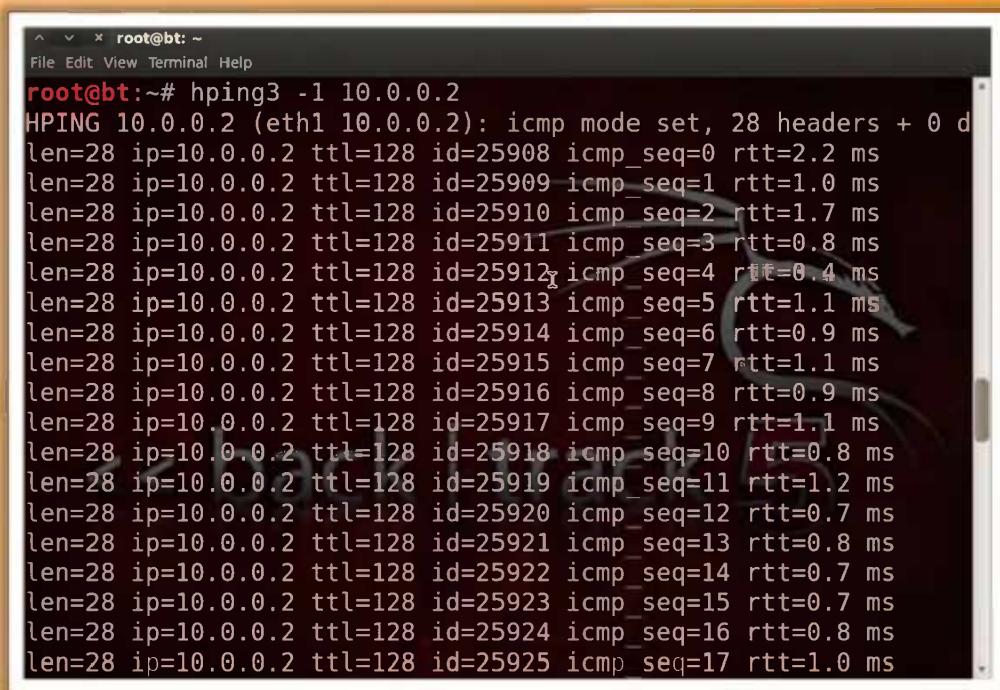
- ➊ Manual path MTU discovery
- ➋ Firewall-like usage allows discovery of open ports behind firewalls
- ➌ Remote OS fingerprinting
- ➍ TCP/IP stack auditing

ICMP Scanning

A ping sweep or **Internet Control Message Protocol (ICMP)** scanning is a process of sending an ICMP request or ping to all hosts on the network to determine which one is up.

This protocol is used by operating system, router, switch, internet-protocol-based devices via the **ping command** to **Echo request** and **Echo response** as a connectivity tester between different hosts.

The following screenshot shows ICMP scanning using the Hping3 tool:



The screenshot shows a terminal window titled "root@bt: ~" with the following command and output:

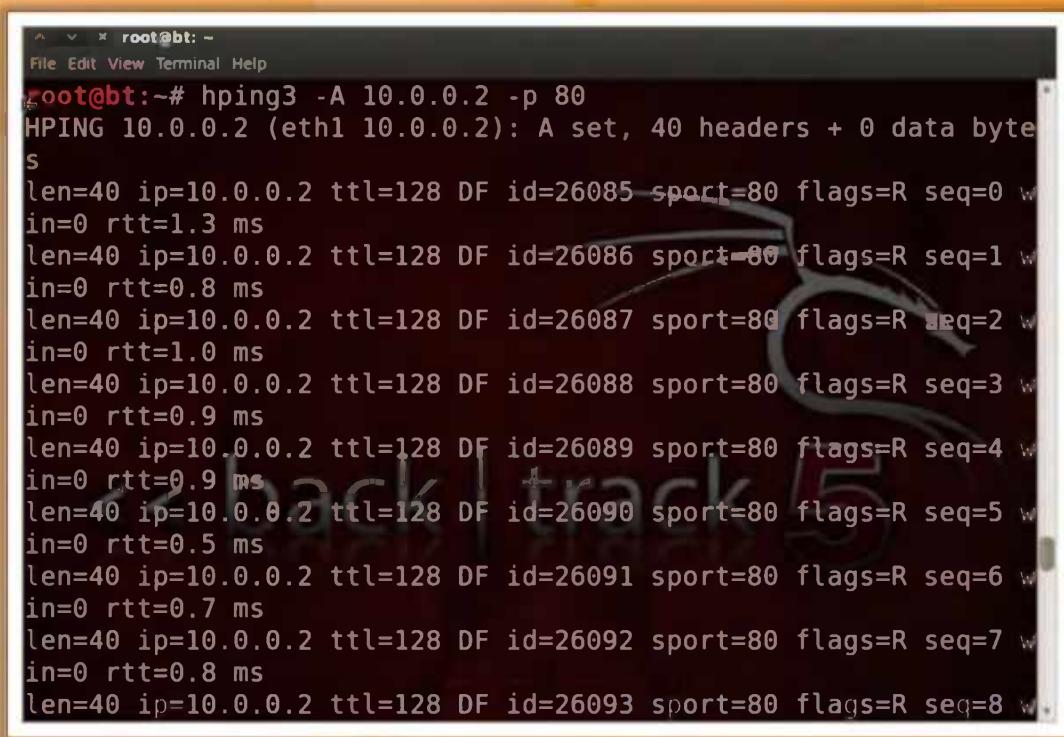
```
root@bt:~# hping3 -1 10.0.0.2
HPING 10.0.0.2 (eth1 10.0.0.2): icmp mode set, 28 headers + 0 d
len=28 ip=10.0.0.2 ttl=128 id=25908 icmp_seq=0 rtt=2.2 ms
len=28 ip=10.0.0.2 ttl=128 id=25909 icmp_seq=1 rtt=1.0 ms
len=28 ip=10.0.0.2 ttl=128 id=25910 icmp_seq=2 rtt=1.7 ms
len=28 ip=10.0.0.2 ttl=128 id=25911 icmp_seq=3 rtt=0.8 ms
len=28 ip=10.0.0.2 ttl=128 id=25912 icmp_seq=4 rtt=0.4 ms
len=28 ip=10.0.0.2 ttl=128 id=25913 icmp_seq=5 rtt=1.1 ms
len=28 ip=10.0.0.2 ttl=128 id=25914 icmp_seq=6 rtt=0.9 ms
len=28 ip=10.0.0.2 ttl=128 id=25915 icmp_seq=7 rtt=1.1 ms
len=28 ip=10.0.0.2 ttl=128 id=25916 icmp_seq=8 rtt=0.9 ms
len=28 ip=10.0.0.2 ttl=128 id=25917 icmp_seq=9 rtt=1.1 ms
len=28 ip=10.0.0.2 ttl=128 id=25918 icmp_seq=10 rtt=0.8 ms
len=28 ip=10.0.0.2 ttl=128 id=25919 icmp_seq=11 rtt=1.2 ms
len=28 ip=10.0.0.2 ttl=128 id=25920 icmp_seq=12 rtt=0.7 ms
len=28 ip=10.0.0.2 ttl=128 id=25921 icmp_seq=13 rtt=0.8 ms
len=28 ip=10.0.0.2 ttl=128 id=25922 icmp_seq=14 rtt=0.7 ms
len=28 ip=10.0.0.2 ttl=128 id=25923 icmp_seq=15 rtt=0.7 ms
len=28 ip=10.0.0.2 ttl=128 id=25924 icmp_seq=16 rtt=0.8 ms
len=28 ip=10.0.0.2 ttl=128 id=25925 icmp_seq=17 rtt=1.0 ms
```

FIGURE 3.12: Hping3 tool showing ICMP scanning output

ACK Scanning on Port 80

You can use this scan technique to probe for the existence of a firewall and its rule sets. Simple packet filtering will allow you to establish connection (packets with the ACK bit set), whereas a sophisticated stateful firewall will not allow you to establish a connection.

The following screenshot shows ACK scanning on port 80 using the Hping3 tool:



The screenshot shows a terminal window titled "root@bt: ~" running on a Backtrack 5 system. The user has run the command "hping3 -A 10.0.0.2 -p 80". The output displays a series of TCP SYNACK packets being sent to the target host at port 80. Each packet is detailed with its length (len=40), source IP (ip=10.0.0.2), TTL (ttl=128), ID (id), sequence number (seq), flags (R for SYN-ACK), and round-trip time (rtt). The sequence numbers range from 80 to 88, indicating a scan of ports 80 through 88.

```
root@bt:~# hping3 -A 10.0.0.2 -p 80
HPING 10.0.0.2 (eth1 10.0.0.2): A set, 40 headers + 0 data bytes
s
len=40 ip=10.0.0.2 ttl=128 DF id=26085 sport=80 flags=R seq=0 w
in=0 rtt=1.3 ms
len=40 ip=10.0.0.2 ttl=128 DF id=26086 sport=80 flags=R seq=1 w
in=0 rtt=0.8 ms
len=40 ip=10.0.0.2 ttl=128 DF id=26087 sport=80 flags=R seq=2 w
in=0 rtt=1.0 ms
len=40 ip=10.0.0.2 ttl=128 DF id=26088 sport=80 flags=R seq=3 w
in=0 rtt=0.9 ms
len=40 ip=10.0.0.2 ttl=128 DF id=26089 sport=80 flags=R seq=4 w
in=0 rtt=0.9 ms
len=40 ip=10.0.0.2 ttl=128 DF id=26090 sport=80 flags=R seq=5 w
in=0 rtt=0.5 ms
len=40 ip=10.0.0.2 ttl=128 DF id=26091 sport=80 flags=R seq=6 w
in=0 rtt=0.7 ms
len=40 ip=10.0.0.2 ttl=128 DF id=26092 sport=80 flags=R seq=7 w
in=0 rtt=0.8 ms
len=40 ip=10.0.0.2 ttl=128 DF id=26093 sport=80 flags=R seq=8 w
```

FIGURE 3.13: Hping3 tool showing ACK scanning output

Hping Commands

CEH Certified Ethical Hacker

ICMP Ping	<code>hping3 -1 10.0.0.25</code>
SYN scan on port 50-60	<code>hping3 -8 50-56 -S 10.0.0.25 -V</code>
ACK scan on port 80	<code>hping3 -A 10.0.0.25 -p 80</code>
FIN, PUSH and URG scan on port 80	<code>hping3 -F -p -U 10.0.0.25 -p 80</code>
UDP scan on port 80	<code>hping3 -2 10.0.0.25 -p 80</code>
Scan entire subnet for live host	<code>hping3 -1 10.0.1.x --rand-dest -I eth0</code>
Collecting Initial Sequence Number	<code>hping3 192.168.1.103 -Q -p 139 -s</code>
Intercept all traffic containing HTTP signature	<code>hping3 -9 HTTP -I eth0</code>
Firewalls and Time Stamps	<code>hping3 -S 72.14.207.99 -p 80 --tcp-timestamp</code>
SYN flooding a victim	<code>hping3 -S 192.168.1.1 -a 192.168.1.254 -p 22 --flood</code>

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

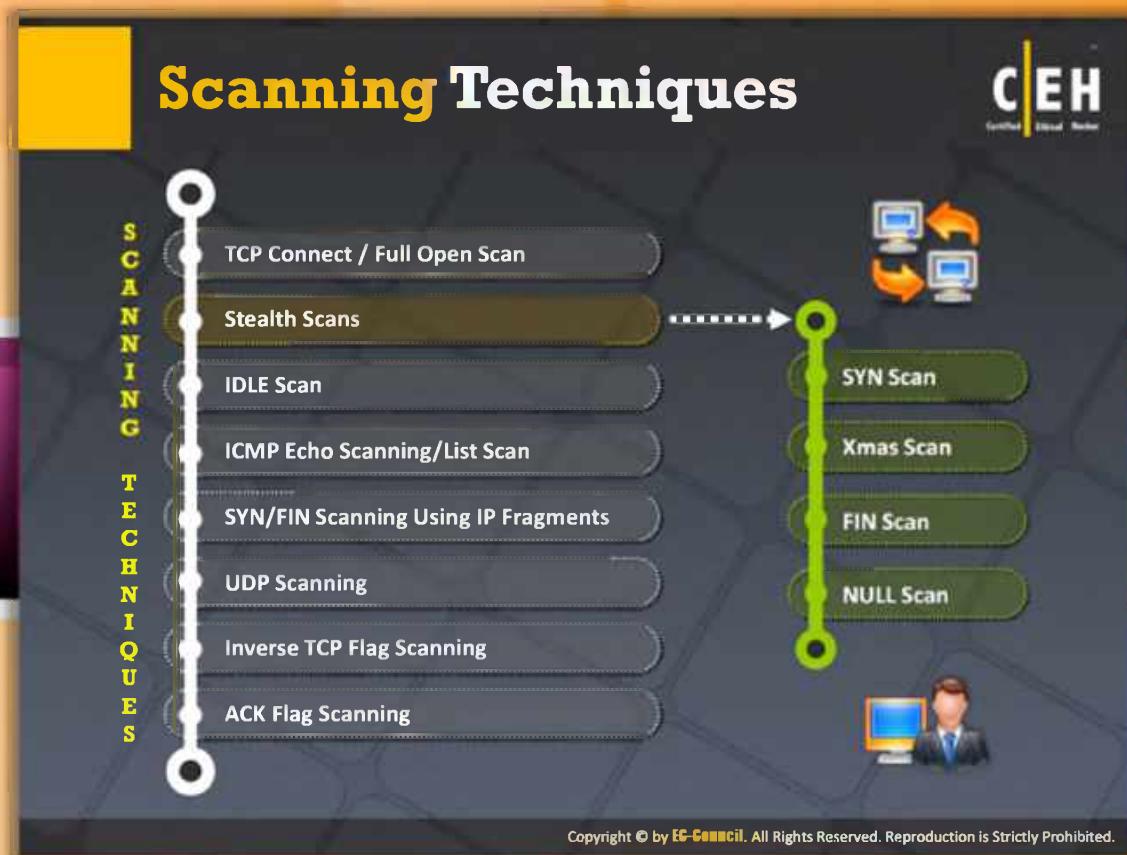


Hping Commands

The following table lists various scanning methods and respective Hping commands:

Scan	Commands
ICMP ping	<code>hping3 -1 10.0.0.25</code>
ACK scan on port 80	<code>hping3 -A 10.0.0.25 -p 80</code>
UDP scan on port 80	<code>hping3 -2 10.0.0.25 -p 80</code>
Collecting initial sequence number	<code>hping3 192.168.1.103 -Q -p 139 -s</code>
Firewalls and time stamps	<code>hping3 -S 72.14.207.99 -p 80 --tcp-timestamp</code>
SYN scan on port 50-60	<code>hping3 -8 50-56 -S 10.0.0.25 -V</code>
FIN, PUSH and URG scan on port 80	<code>hping3 -F -p -U 10.0.0.25 -p 80</code>
Scan entire subnet for live host	<code>hping3 -1 10.0.1.x --rand-dest -I eth0</code>
Intercept all traffic containing HTTP signature	<code>hping3 -9 HTTP -I eth0</code>
SYN flooding a victim	<code>hping3 -S 192.168.1.1 -a 192.168.1.254 -p 22 --flood</code>

TABLE 3.1: Hping Commands Table



Scanning Techniques

Scanning is the process of **gathering information** about the systems that are alive and responding on the network.

The **port scanning techniques** are designed to identify the open ports on a targeted server or host. This is often used by administrators to verify security policies of their networks and by attackers to identify running services on a host with the intent of compromising it.

Different types of scanning techniques employed include:

- ⌚ TCP Connect / Full Open Scan
- ⌚ Stealth Scans: SYN Scan (Half-open Scan); XMAS Scan, FIN Scan, NULL Scan
- ⌚ IDLE Scan
- ⌚ ICMP Echo Scanning/List Scan
- ⌚ SYN/FIN Scanning Using IP Fragments
- ⌚ UDP Scanning
- ⌚ Inverse TCP Flag Scanning
- ⌚ ACK Flag Scanning

The following is the list of important reserved ports:

Name	Port/Protocol	Description
echo	7/tcp	
echo	7/udp	
discard	9/tcp	sink null
discard	9/udp	sink null
systat	11/tcp	Users
daytime	13/tcp	
daytime	13/udp	
netstat	15/tcp	
qotd	17/tcp	Quote
chargen	19/tcp	ttytst source
chargen	19/udp	ttytst source
ftp-data	20/tcp	ftp data transfer
ftp	21/tcp	ftp command
ssh	22/tcp	Secure Shell
telnet	23/tcp	
smtp	25/tcp	Mail
time	37/tcp	Timeserver
time	37/udp	Timeserver
rlp	39/udp	resource location
nicname	43/tcp	who is
domain	53/tcp	domain name server
domain	53/udp	domain name server
sql*net	66/tcp	Oracle SQL*net
sql*net	66/udp	Oracle SQL*net
bootps	67/tcp	bootp server
bootps	67/udp	bootp server
bootpc	68/tcp	bootp client

Name	Port/Protocol	Description
bootpc	68/udp	bootp client
tftp	69/tcp	Trivial File Transfer
tftp	69/udp	Trivial File Transfer
gopher	70/tcp	gopher server
finger	79/tcp	Finger
www-http	80/tcp	WWW
www-http	80/udp	WWW
kerberos	88/tcp	Kerberos
kerberos	88/udp	Kerberos
pop2	109/tcp	PostOffice V.2
Pop3	110/tcp	PostOffice V.3
sunrpc	111/tcp	RPC 4.0 portmapper
sunrpc	111/udp	RPC 4.0 portmapper
auth/ident	113/tcp	Authentication Service
auth	113/udp	Authentication Service
audionews	114/tcp	Audio News Multicast
audionews	114/udp	Audio News Multicast
nntp	119/tcp	Usenet Network News Transfer
nntp	119/udp	Usenet Network News Transfer
ntp	123/tcp	Network Time Protocol
ntp	123/udp	Network Time Protocol
netbios-ns	137/tcp	NETBIOS Name Service
netbios-ns	137/udp	NETBIOS Name Service
netbios-dgm	138/tcp	NETBIOS Datagram Service
netbios-dgm	138/udp	NETBIOS Datagram Service
netbios-ssn	139/tcp	NETBIOS Session Service
netbios-ssn	139/udp	NETBIOS Session Service
imap	143/tcp	Internet Message Access Protocol

imap	143/udp	Internet Message Access Protocol
sql-net	150/tcp	SQL-NET
sql-net	150/udp	SQL-NET
sqlsrv	156/tcp	SQL Service
sqlsrv	156/udp	SQL Service
snmp	161/tcp	
snmp	161/udp	
snmp-trap	162/tcp	
snmp-trap	162/udp	
cmip-man	163/tcp	CMIP/TCP Manager
cmip-man	163/udp	CMIP
cmip-agent	164/tcp	CMIP/TCP Agent
cmip-agent	164/udp	CMIP
irc	194/tcp	Internet Relay Chat
irc	194/udp	Internet Relay Chat
at-rtmp	201/tcp	AppleTalk Routing Maintenance
at-rtmp	201/udp	AppleTalk Routing Maintenance
at-nbp	202/tcp	AppleTalk Name Binding
at-nbp	202/udp	AppleTalk Name Binding
at-3	203/tcp	AppleTalk
at-3	203/udp	AppleTalk
at-echo	204/tcp	AppleTalk Echo
at-echo	204/udp	AppleTalk Echo
at-5	205/tcp	AppleTalk
at-5	205/udp	AppleTalk
at-zis	206/tcp	AppleTalk Zone Information
at-zis	206/udp	AppleTalk Zone Information
at-7	207/tcp	AppleTalk

at-7	207/udp	AppleTalk
at-8	208/tcp	AppleTalk
at-8	208/udp	AppleTalk
ipx	213/tcp	
ipx	213/udp	
imap3	220/tcp	Interactive Mail Access Protocol v3
imap3	220/udp	Interactive Mail Access Protocol v3
aurp	387/tcp	AppleTalk Update-Based Routing
aurp	387/udp	AppleTalk Update-Based Routing
netware-ip	396/tcp	Novell Netware over IP
netware-ip	396/udp	Novell Netware over IP
Name	Port/Protocol	Description
rmt	411/tcp	Remote mt
rmt	411/udp	Remote mt
54erberos54-ds	445/tcp	
54erberos54-ds	445/udp	
isakmp	500/udp	ISAKMP/IKE
fcp	510/tcp	First Class Server
exec	512/tcp	BSD rexecd(8)
comsat/biff	512/udp	used by mail system to notify users
login	513/tcp	BSD rlogind(8)
who	513/udp	whod BSD rwhod(8)
shell	514/tcp	cmd BSD rshd(8)
syslog	514/udp	BSD syslogd(8)
printer	515/tcp	spooler BSD lpd(8)
printer	515/udp	Printer Spooler
talk	517/tcp	BSD talkd(8)
talk	517/udp	Talk
ntalk	518/udp	New Talk (ntalk)

ntalk	518/udp	SunOS talkd(8)
netnews	532/tcp	Readnews
uucp	540/tcp	uucpd BSD uucpd(8)
uucp	540/udp	uucpd BSD uucpd(8)
klogin	543/tcp	Kerberos Login
klogin	543/udp	Kerberos Login
kshell	544/tcp	Kerberos Shell
kshell	544/udp	Kerberos Shell
ekshell	545/tcp	krcmd Kerberos encrypted remote shell –kfall
pcserver	600/tcp	ECD Integrated PC board srvr
mount	635/udp	NFS Mount Service
pcnfs	640/udp	PC-NFS DOS Authentication
bwnfs	650/udp	BW-NFS DOS Authentication
flexlm	744/tcp	Flexible License Manager
flexlm	744/udp	Flexible License Manager
56erberos-adm	749/tcp	Kerberos Administration
56erberos-adm	749/udp	Kerberos Administration
kerberos	750/tcp	kdc Kerberos authentication—tcp
kerberos	750/udp	Kerberos
56erberos_master	751/udp	Kerberos authentication
56erberos_master	751/tcp	Kerberos authentication
krb_prop	754/tcp	Kerberos slave propagation

	999/udp	Applixware
socks	1080/tcp	
socks	1080/udp	
kpop	1109/tcp	Pop with Kerberos
ms-sql-s	1433/tcp	Microsoft SQL Server
ms-sql-s	1433/udp	Microsoft SQL Server
ms-sql-m	1434/tcp	Microsoft SQL Monitor
ms-sql-m	1434/udp	Microsoft SQL Monitor
Name	Port/Protocol	Description
pptp	1723/tcp	Pptp
pptp	1723/udp	Pptp
nfs	2049/tcp	Network File System
nfs	2049/udp	Network File System
eklogin	2105/tcp	Kerberos encrypted rlogin
rkinit	2108/tcp	Kerberos remote kinit
kx	2111/tcp	X over Kerberos
kauth	2120/tcp	Remote kauth
lyskom	4894/tcp	LysKOM (conference system)
sip	5060/tcp	Session Initiation Protocol
sip	5060/udp	Session Initiation Protocol
x11	6000-6063/tcp	X Window System
x11	6000-6063/udp	X Window System
irc	6667/tcp	Internet Relay Chat
afs	7000-7009/udp	
afs	7000-7009/udp	

TABLE 3.2: Reserved Ports Table

TCP Connect / Full Open Scan

 CEH Certified Ethical Hacker

- TCP Connect scan detects when a port is open by completing the **three-way handshake**
- TCP Connect scan **establishes a full connection** and tears it down by sending a **RST packet**

Scan result when a port is open



Scan result when a port is closed



Screenshot of ZMap tool showing scan results:

```
Starting Nmap 7.00 ( http://nmap.org ) at 2015-09-28 22:49 UTC
Nmap scan type: SYN+ACK
Nmap version: 7.00 ( http://nmap.org )
```

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



TCP Connect / Full Open Scan

Source: <http://www.insecure.org>

TCP Connect / Full Open Scan is one of the most **reliable** forms of **TCP scanning**. The TCP connect() system call provided by an OS is used to open a connection to every interesting port on the machine. If the port is listening, connect() will succeed; otherwise, the port isn't reachable.



TCP Three-way Handshake

In the TCP three-way handshake, the client sends a **SYN flag**, which is acknowledged by a **SYN+ACK flag** by the server which, in turn, is acknowledged by the client with an ACK flag to complete the connection. You can establish a connection from both ends, and terminate from both ends individually.



Vanilla Scanning

In vanilla scanning, once the handshake is completed, the client ends the connection. If the connection is not established, then the scanned machine will be **Dos'd**, which allows you to make a new socket to be **created/called**. This confirms you with an open port to be scanned for a running service. The process will continue until the maximum port threshold is reached.

If the port is closed the server responds with an RST+ACK flag (RST stands for “**Reset the connection**”), whereas the client responds with a RST flag and here ends the connection. This is created by a TCP connect () system call and will be identified instantaneously if the port is opened or closed.

Making separate connects() call for every targeted port in a linear fashion would take a long time over a slow connection. The attacker can accelerate the scan by using many sockets in parallel. Using non-blocking, I/O allows the attacker to set a low time-out period and watch all the sockets simultaneously.



Disadvantages

The drawback of this type of scan is **easily detectable** and **filterable**. The logs in the target system will disclose the connection.

The Output

Initiating Connect () Scan against (172.17.1.23)

Adding open port 19/tcp

Adding open port 21/tcp

Adding open port 13/tcp



FIGURE 3.14: Scan results when a port is open



FIGURE 3.15: Scan results when a port is closed

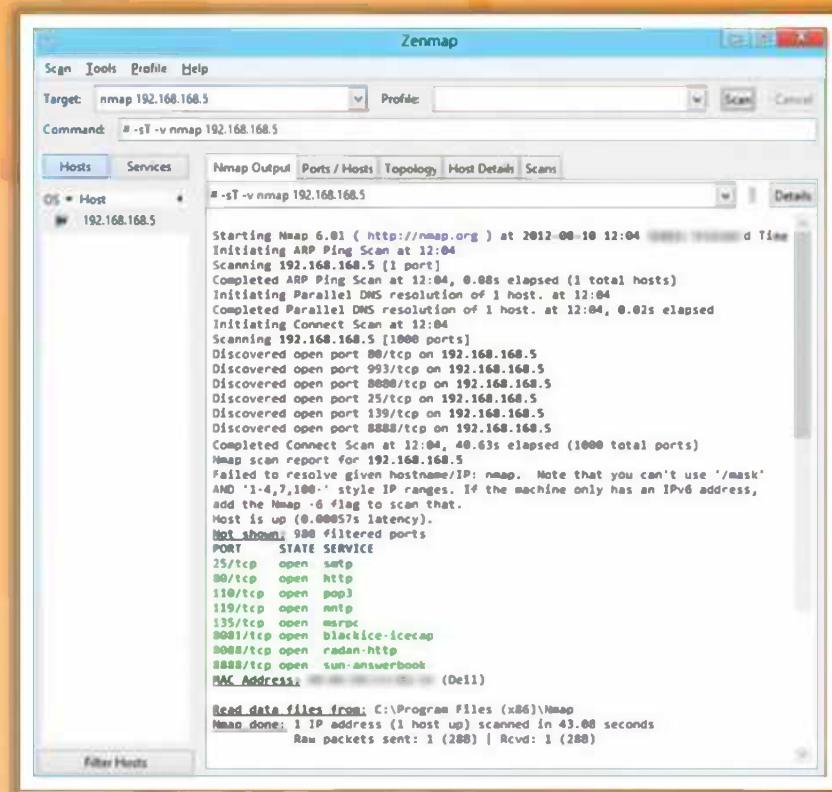


FIGURE 3.16: Zenmap Screenshot

Stealth Scan (Half-open Scan)

Attackers use stealth scanning techniques to **bypass firewall rules, logging mechanism, and hide themselves as usual network traffic**

Stealth Scan Process

- 1 The client sends a single **SYN** packet to the server on the appropriate port
- 2 If the port is open then the server responds with a **SYN/ACK** packet
- 3 If the server responds with an **RST** packet, then the remote port is in the "closed" state
- 4 The client sends the **RST** packet to close the initiation before a connection can ever be established

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



Stealth Scan (Half-Open Scan)

Stealth scan sends a **single frame** to a **TCP port** without any TCP handshaking or additional packet transfers. This is a scan type that sends a single frame with the expectation of a single response. The half-open scan partially opens a connection, but stops halfway through. This is also known as a **SYN scan** because it only sends the **SYN packet**. This stops the service from ever being notified of the incoming connection. **TCP SYN** scans or half-open scanning is a stealth method of port scanning.

The three-way handshake methodology is also implemented by the stealth scan. The difference is that in the last stage, remote ports are identified by examining the packets entering the interface and terminating the connection before a new initialization was triggered.

The process preludes the following:

- >To start initialization, the client forwards a single "**SYN**" packet to the destination server on the corresponding port.
- The server actually initiates the stealth scanning process, depending on the response sent.
- If the server forwards a "**SYN/ACK**" response packet, then the port is supposed to be in an "**OPEN**" state.

If the response is forwarded with an "RST" packet, then the port is supposed to be in a "CLOSED" state.



FIGURE 3.16: Stealth Scan when Port is Open



FIGURE 3.17: Stealth Scan when Port is Closed

Zenmap Tool

Zenmap is the official **graphical user interface (GUI)** for the **Nmap** Security Scanner. Using this tool you can save the frequently used scans as profiles to make them easy to run recurrently. It contains a command creator that allows you to interact and create Nmap command lines. You can save the Scan results and view them in the future and they can be compared with another scan report to locate differences. The results of the recent scans can be stored in a **searchable database**.

The advantages of Zenmap are as follows:

- ⌚ Interactive and graphical results viewing
- ⌚ Comparison
- ⌚ Convenience
- ⌚ Repeatability
- ⌚ Discoverability

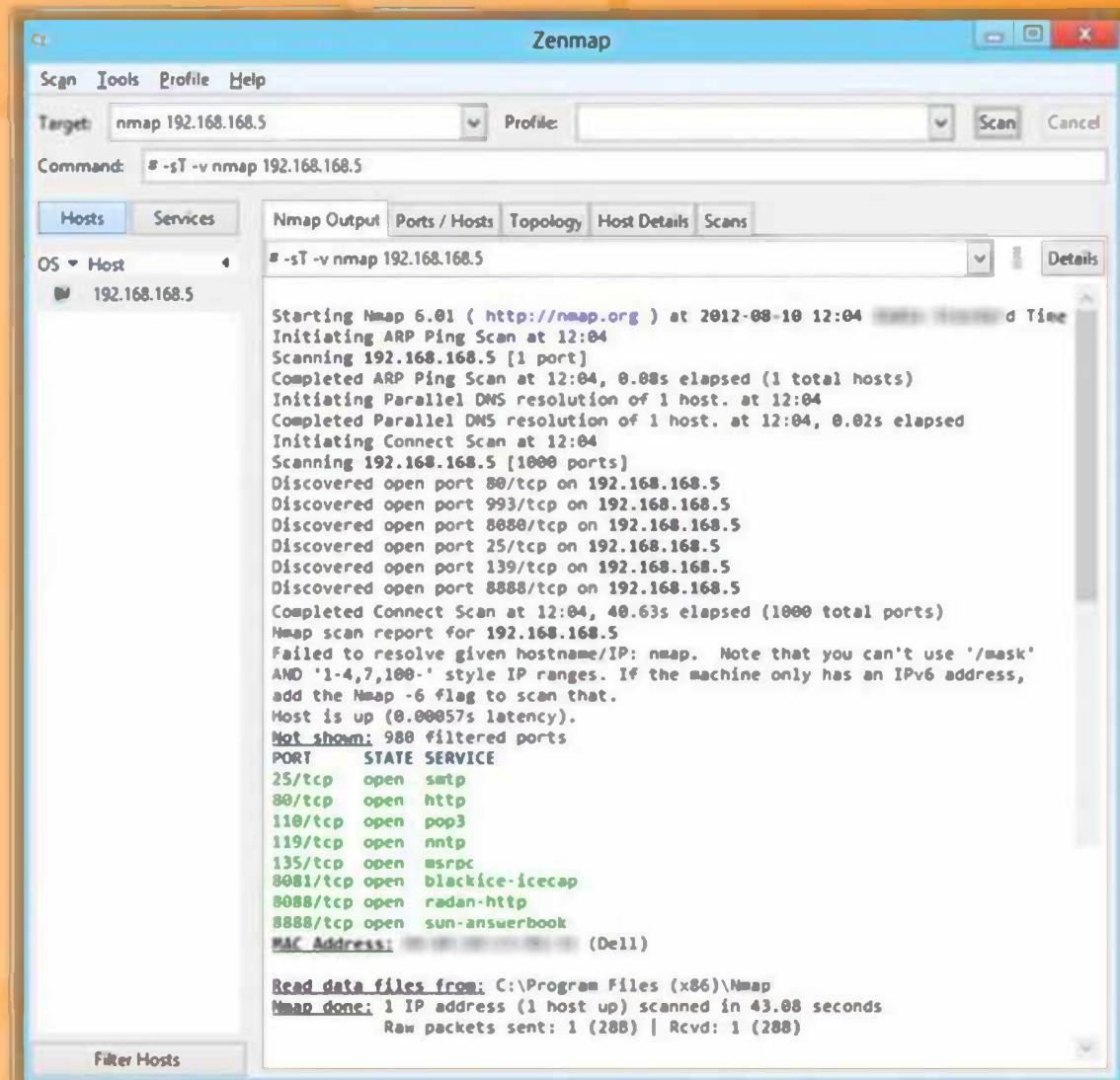


FIGURE 3.18: Zenmap Showing Scanning Results

Xmas Scan

Port is open

Port is closed

- In Xmas scan, attackers send a TCP frame to a remote device with **URG, ACK, RST, SYN, PSH, and FIN** flags set
- FIN scan only with OS TCP/IP developed according to **RFC 793**
- It will not work against any current version of **Microsoft Windows**

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



Xmas Scan

Xmas Scan is a **port scan technique** with ACK, RST, SYN, URG, PSH, and FIN flags set to send a TCP frame to a remote device. If the target port is closed, then you will receive a remote system reply with a RST. You can use this port scan technique to scan large networks and find which host is up and what services it is offering. It is a technique to describe all TCP flag sets. When all flags are set, some systems hang; so the flags most often set are the nonsense pattern URG-PSH-FIN. This scan only works when systems are compliant with RFC 793.



BSD Networking Code

This method is based on BSD networking code; you can use this only for **UNIX hosts** and it does not support Windows NT. If this scan is directed at any Microsoft system, it shows all the ports on the host are opened.



Transmitting Packets

You can initialize all the flags when transmitting the packet to a remote host. If the target system accepts packet and does not send any response, the port is open. If the target system sends RST flag, the port is closed.

Advantage:

It avoids the IDS and TCP three-way handshake.

Disadvantage:

It works on the UNIX platform only.



FIGURE 3.19: Xmas Scan when Port is Open



FIGURE 3.20: Xmas Scan when Port is Closed

Zenmap is the official graphical user interface (GUI) for the **Nmap Security Scanner**. Using this tool you can **save** the frequently used **scans** as **profiles** to make them easy to run recurrently.

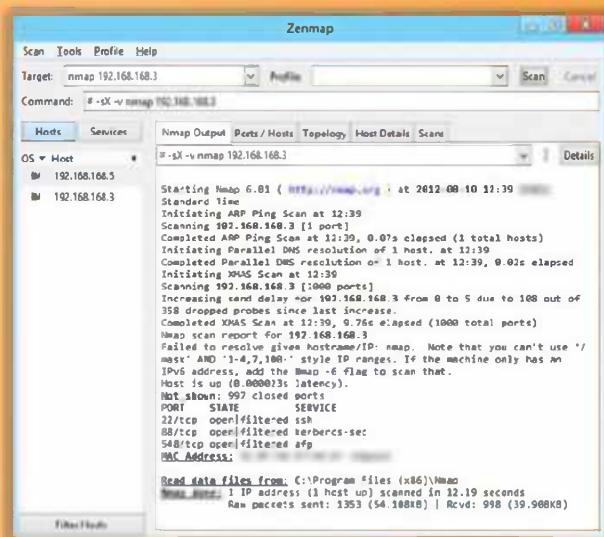


FIGURE 3.21: Zenmap Showing Xmas Scan Result

FIN Scan

C|EH
Certified Ethical Hacker

- In FIN scan, attackers send a TCP frame to a remote host with only FIN flags set
- FIN scan only with OS TCP/IP developed according to **RFC 793**
- It will not work against any current version of **Microsoft Windows**

The diagram illustrates the FIN Scan process. It shows two scenarios: 1) If the port is open, the server returns 'No Response'. 2) If the port is closed, the server returns an 'RST/ACK' response. To the right, a screenshot of the NetworkMiner tool interface shows a captured FIN packet and its corresponding response.

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



FIN Scan

FIN Scan is a type of port scan. The client sends a **FIN packet** to the target port, and if the service is not running or if the port is closed it replies to you with the probe packet with an RST.



FIGURE 3.22: FIN Scan when Port is Open



FIGURE 3.23: FIN Scan when Port is Closed

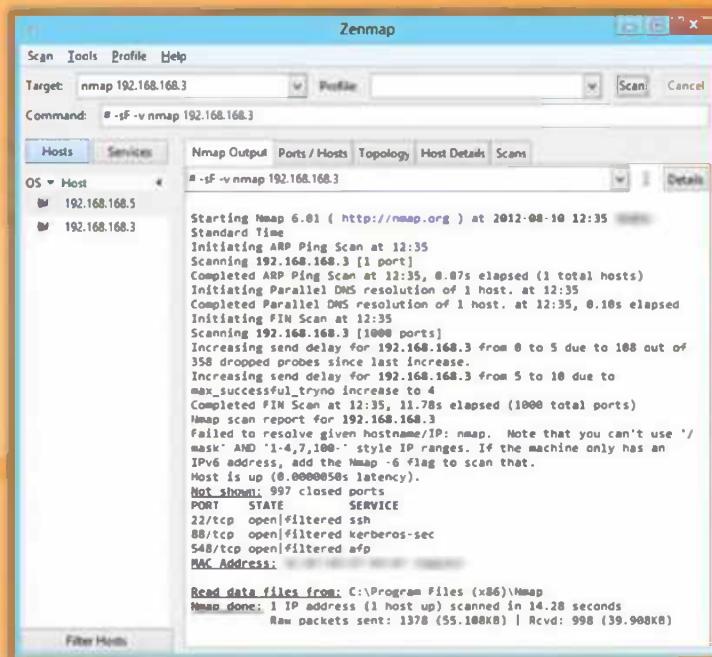


FIGURE 3.24: Zenmap showing FIN Scan Result

NULL Scan

Port Is open

Attacker 10.0.0.6 → TCP Packet with NO Flag Set → Server 10.0.0.8:23 → No Response

Port is closed

Attacker 10.0.0.6 → TCP Packet with NO Flag Set → Server 10.0.0.8:23 → RST/ACK

- In NULL scan, attackers send a TCP frame to a remote host with **NO Flags**
- NULL scan only works if OS' TCP/IP implementation is developed according to **RFC 793**
- It will not work against any current version of **Microsoft Windows**

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



NULL Scan

NULL scans send TCP packets with **all flags turned off**. It is assumed that closed ports will return a TCP RST. Packets received by open ports are discarded as invalid.

It sets all flags of TCP headers, such as ACK, FIN, RST, SYN, URG and PSH, to NULL or unassigned. When any packets arrive at the server, BSD networking code informs the kernel to drop the incoming packet if a port is open, or returns an RST flag if a port is closed. This scan uses flags in the reverse fashion as the Xmas scan, but gives the same output as FIN and Xmas tree scans.

Many network codes of major operating systems can behave differently in terms of responding to the packet, e.g., Microsoft versus UNIX. This method does not work for Microsoft operating systems.

Command line option for null scanning with NMAP is “-sN”

Advantage:

It avoids IDS and TCP three-way handshake.

Disadvantage:

It works only for UNIX.



FIGURE 3.25: NULL Scan when Port is Open

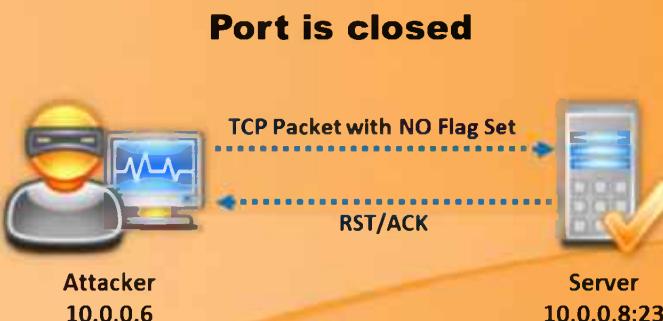


FIGURE 3.26: NULL Scan when Port is Closed

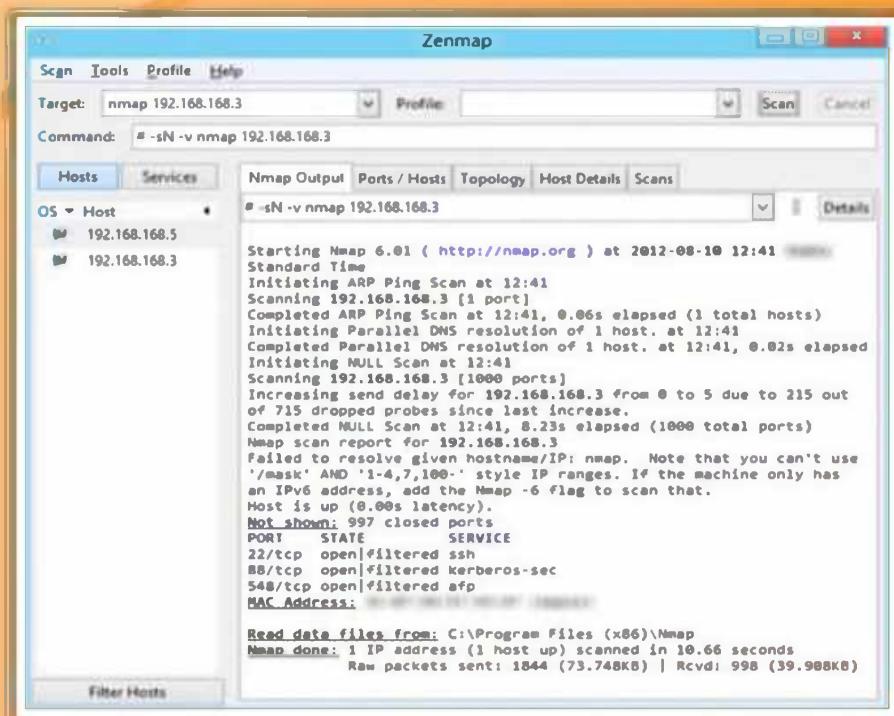


FIGURE 3.27: Zenmap showing NULL Scan Result

IDLE Scan

The CEH logo is in the top right corner.

Most network servers listen on TCP ports, such as web servers on port 80 and mail servers on port 25. Port is considered "open" if an application is listening on the port

One way to determine whether a port is open is to send a "SYN" (session establishment) packet to the port

The target machine will send back a "SYN|ACK" (session request acknowledgment) packet if the port is open, and an "RST" (Reset) packet if the port is closed

A machine that receives an unsolicited SYN|ACK packet will respond with an RST. An unsolicited RST will be ignored

Every IP packet on the Internet has a "fragment identification" number (IP ID)

OS increments the IP ID for each packet sent, thus probing an IP ID gives an attacker the number of packets sent since last probe

Command Prompt

```
C:\>nmap -Pn -p- -sI www.juggyboy.com www.certifiedhacker.com
Starting Nmap ( http://nmap.org )
IdleScan using zombie www.juggyboy.com (192.130.18.124:80); Class: Incremental
Nmap scan report for 198.182.30.110
(The 40321 ports scanned but not shown below are in state: closed)
Port      State       Service
21/tcp    open        ftp
25/tcp    open        smtp
80/tcp    open        http
Nmap done: 1 IP address (1 host up) scanned in 1931.23 seconds
```

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



IDLE Scan

The idle scan is a **TCP port scan** method that you can use to send a spoofed source address to a computer to find out what services are available and offers complete blind scanning of a remote host. This is accomplished by impersonating another computer. No packet is sent from your own IP address; instead, another host is used, often called a "**zombie**," to scan the remote host and determine the open ports. This is done by expecting the sequence numbers of the zombie host and if the remote host checks the IP of the scanning party, the IP of the zombie machine will show up.

Understanding TCP/IP

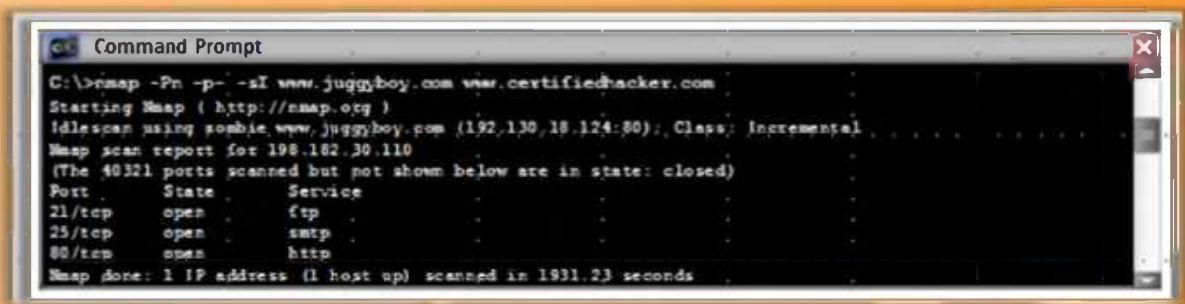
Source: <http://nmap.org>

Idle scanning is a sophisticated port scanning method. You do not need to be a TCP/IP expert to understand it. You need to understand the following basic facts:

- Most of the network servers listen on TCP ports, such as web servers on port 80 and mail servers on port 25. A port is considered "open" if an application is listening on the port; otherwise it is closed.

- ➊ To determine whether a port is open, send a session establishment "SYN" packet to the port. The target machine responds with a session request acknowledgment "SYN|ACK" packet if the port is open and a Reset "RST" packet if the port is closed.
- ➋ A machine that receives an unsolicited SYN|ACK packet responds with an RST. An unsolicited RST is ignored.
- ➌ Every IP packet on the Internet has a "fragment identification" number. Many operating systems simply increment this number for every packet they send. So probing for this number can tell an attacker how many packets have been sent since the last probe.

From these facts, it is possible to scan a target network while forging your identity so that it looks like an innocent "zombie" machine did the scanning.



The screenshot shows a Windows Command Prompt window titled "Command Prompt". The command entered is "C:\>nmap -Pn -sI www.jugglyboy.com www.certifiedhacker.com". The output shows an idle scan using a zombie host at 192.130.18.124:80. It lists ports 21/tcp (open), 25/tcp (open), and 80/tcp (open) as being in state "closed". The scan took 1931.23 seconds.

```
C:\>nmap -Pn -sI www.jugglyboy.com www.certifiedhacker.com
Starting Nmap ( http://nmap.org )
IdleScan using zombie www.jugglyboy.com (192.130.18.124:80); Class: Incremental
Nmap scan report for 198.182.30.110
(The 40321 ports scanned but not shown below are in state: closed)
Port      State       Service
21/tcp    open        ftp
25/tcp    open        smtp
80/tcp    open        http
Nmap done: 1 IP address (1 host up) scanned in 1931.23 seconds
```

FIGURE 3.28: Nmap Showing Idle Scan Result

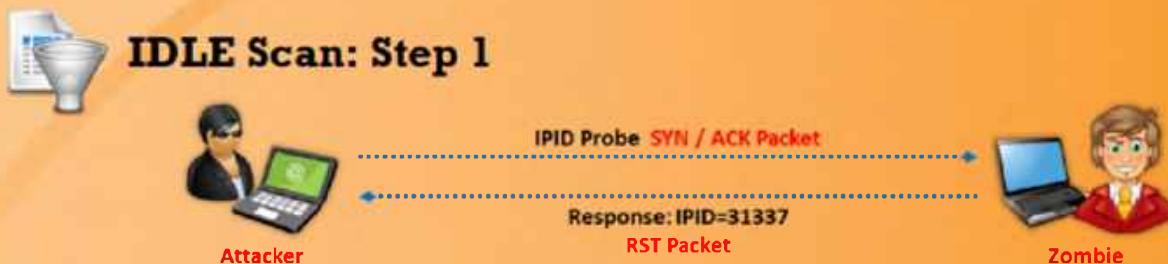
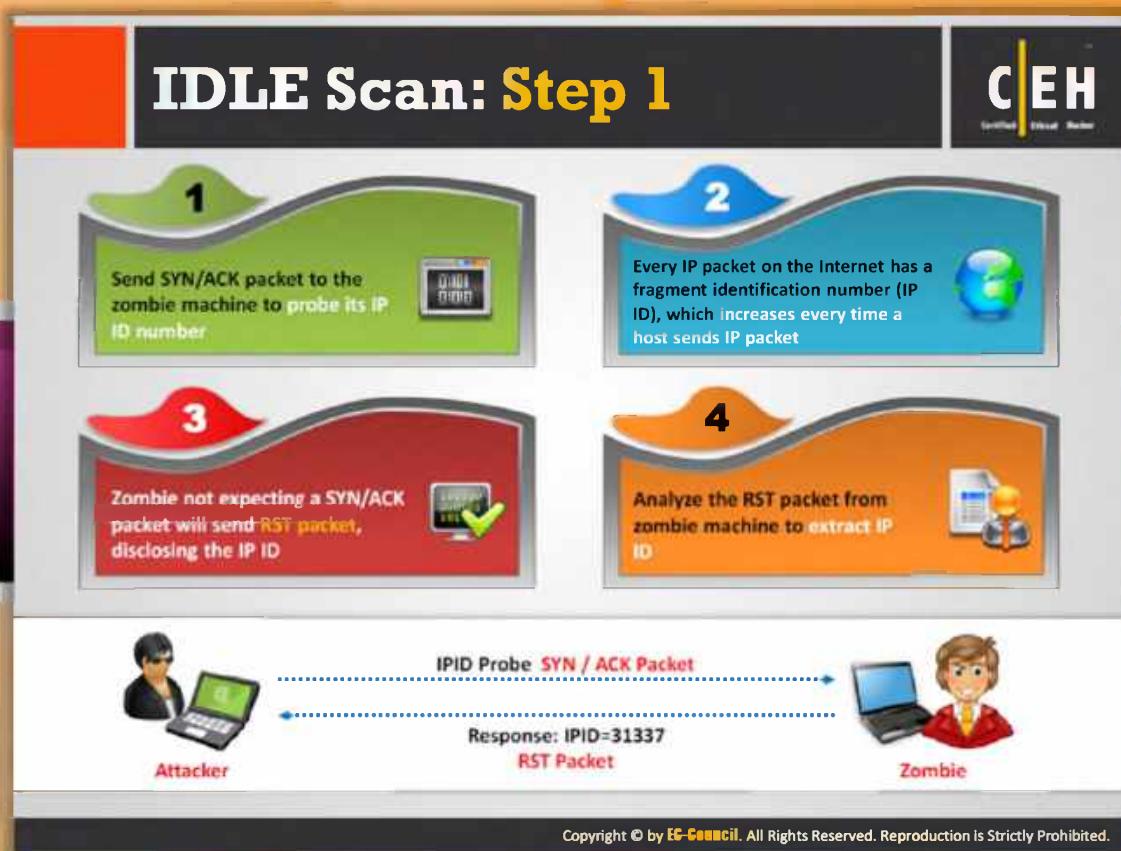


FIGURE 3.29: IPID Probe Request and Response

Choose a "Zombie" and Probe for its Current IP Identification (IPID) Number

In the first step, you can send a session establishment "SYN" packet or IPID probe to determine whether a port is open or closed. If the port is open, the "zombie" responds with a session request acknowledgment "SYN|ACK" packet containing the IPID of the remote host machine. If the port is closed, it sends a reset "RST" packet. Every IP packet on the Internet has a "fragment identification" number, which is incremented by one for every packet transmission. In the above diagram, the zombie responds with **IPID=31337**.

IDLE Scan: Step 2 and 3

Step 2

- Send SYN packet to the target machine (port 80) spoofing the IP address of the “zombie”
- If the port is open, the target will send SYN/ACK Packet to the zombie and in response zombie sends RST to the target
- If the port is closed, the target will send RST to the “zombie” but zombie will not send anything back

Step 3

- Probe “zombie” IPID again

IDLE Scan: Step 2 and 3



Idle Scan: Step 2.1 (Open Port)

Send a SYN packet to the target machine (port 80) spoofing the IP address of the “zombie.” If the port is open, the target will send the **SYN/ACK packet** to the zombie and in response the zombie sends the RST to the target.

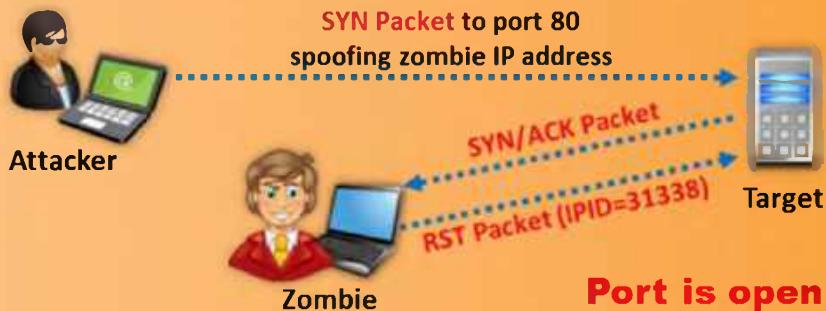


FIGURE 3.30: Target Response to Spoofed SYN Request when Port is Open



Idle Scan: Step 2.2 (Closed Port)

The target will send the RST to the “zombie” if the port is closed, but the zombie will

not send anything back.

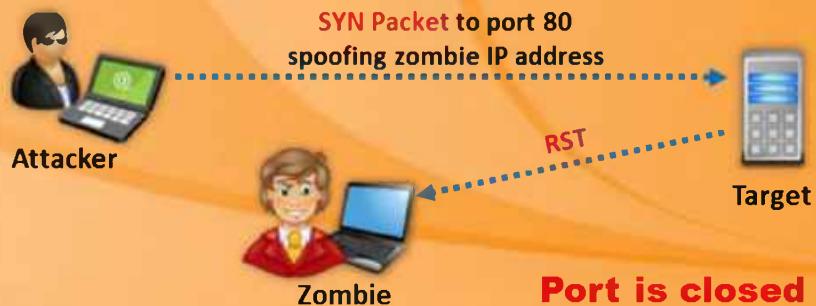


FIGURE 3.31: Target Response to Spoofed SYN Request when Port is Closed



Idle Scan: Step 3

Probe the "zombie" IPID again.



FIGURE 3.32: IPID Probe Request and Response

ICMP Echo Scanning/List Scan

The screenshot shows two windows of the Zenmap interface. The left window is titled 'ICMP Echo Scanning' and displays the output of the command 'nmap -P cert.org/24 152.148.0.0/16'. It shows a single host at 152.148.0.126 with an OS of 'OS: 4 Host'. The right window is titled 'List Scan' and displays the output of 'nmap -sL ~192.168.108.5'. It shows a single host at 192.168.108.5 with an OS of 'OS: 1 Host'. Both windows have tabs for Scan, Tools, Profile, Help, Nmap Output, Ports / Hosts, Topology, Host Details, and Scan.

ICMP Echo Scanning

- This is not really port scanning, since ICMP does not have a port abstraction
- But it is sometimes useful to determine which hosts in a network are up by pinging them all
- `nmap -P cert.org/24 152.148.0.0/16`

List Scan

- This type of scan simply generates and prints a list of IPs/Names without actually pinging or port scanning them
- A DNS name resolution will also be carried out

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



ICMP Echo Scanning/List Scan

ICMP echo scanning is used to **discover live machines by pinging all the machines** in the target network. Attackers send ICMP probes to the broadcast or network address which is relayed to all the host addresses in the subnet. The live systems will send ICMP echo reply message to the source of ICMP echo probe.

ICMP echo scanning is used in UNIX/Linux and BSD-based machines as the TCP/IP stack implementations in these operating system responds to the ICMP echo requests to the broadcast addresses. This technique cannot be used in Windows based networks as the TCP/IP stack implementation in windows machines is configured, by default, not to reply ICMP probes directed to the broadcast address.

ICMP echo scanning is not referred to as **port scanning** since it does not have a port abstraction. ICMP echo scanning is useful to determine which hosts in a network are active by pinging them all. The active hosts in the network is displayed in **Zenmap** as "Host is up (**0.020s latency**).". You can observe that in the screenshot:

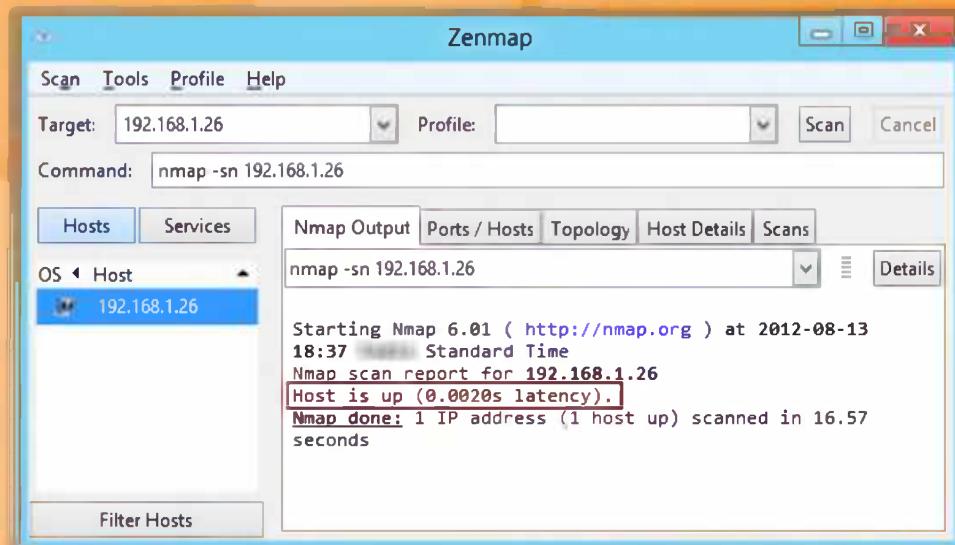


FIGURE 3.33: Zenmap showing ICMP Echo Scanning Result

In a list scan, discovery of the active host in the network is done indirectly. A list scan simply generates and prints a list of IPs/Names without actually pinging the host names or port scanning them. As a result, the list scan output of all the IP addresses will be shown as “not scanned,” i.e., (0 hosts up). By default, a **reverse DNS** resolution is still being carried out on the host by Nmap for learning their names.

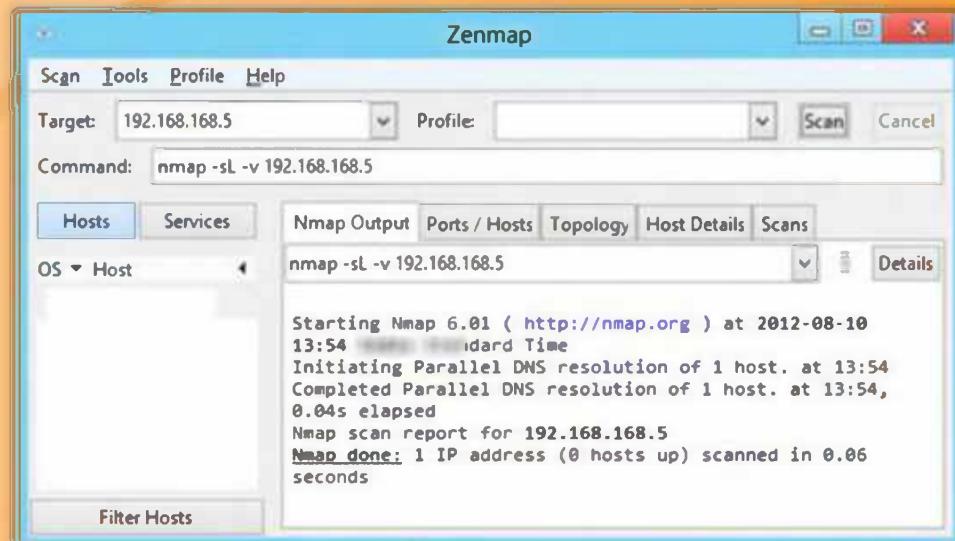


FIGURE 3.34: Zenmap showing List Scanning Result

Advantage:

- ⊕ A list scan can perform a good sanity check.
- ⊕ The incorrectly defined IP addresses on the command line or in an option file are detected by the list scan. The detected errors should be repaired prior to running any “active” scan.

UDP Scanning

Are you **open** on UDP Port 29?

If Port is Closed, an **ICMP Port unreachable** message is received

No response if port is **Open**

Attacker **Server**

UDP Port Open

- There is no **three-way TCP handshake** for UDP scan
- The system does not respond with a message when the port is **open**

UDP Port Closed

- If a UDP packet is sent to **closed** port, the system responds with **ICMP port unreachable message**
- Spywares, Trojan horses, and other malicious applications use UDP ports

CEH Certified Ethical Hacker

UDP Scanning

UDP Raw ICMP Port Unreachable Scanning

UDP port scanners use the **UDP protocol** instead of TCP, and can be more difficult than TCP scanning. You can send a packet, but you cannot determine that the host is alive or dead or filtered. However, there is one ICMP that you can use to determine whether ports are open or closed. If you send a UDP packet to a port without an application bound to it, the IP stack will return an **ICMP port unreachable packet**. If any port returns an ICMP error, then it's closed, while the ports that didn't answer are either open or filtered by the firewall.

This happens because open ports do not have to send an acknowledgement in response to a probe, and closed ports are not even required to send an error packet.

UDP Packets

Source: <http://nmap.org>

When you send a packet to a closed UDP port, most of the hosts send an **ICMP_PORT_UNREACH** error. Thus, you can find out if a port is NOT open. Neither UDP packets nor the ICMP errors are guaranteed to arrive, so UDP scanners of this sort must also implement the retransmission of packets that appear lost. UDP scanners interpret lost traffic as open ports.

In addition, this scanning technique is slow because of limiting the ICMP error message rate as compensation to machines that apply RFC 1812 section 4.3.2.8. A remote host will need to access the raw ICMP socket to distinguish closed from unreachable ports.

UDP RECVFROM () and WRITE () Scanning

While non-root users cannot read port unreachable errors directly; Linux informs you indirectly when they receive messages.

Example

For example, a second write () call to a closed port will usually fail. A lot of scanners, such as Netcat and Pluvial pscan.c do recvfrom () on non-blocking UDP sockets, usually return EAGAIN ("Try Again," errno 13) if the ICMP error has not been received, and ECONNREFUSED ("Connection refused," errno 111), if it has. This is the technique used for determining open ports when non-root users use -u (UDP). Root users can also use the -l (lamer UDP scan) options to force this.

Advantage:

The UDP scan is less informal regarding an open port, since there's no overhead of a TCP handshake. However, if ICMP is responding to each unavailable port, the number of total frames can exceed a TCP scan. Microsoft-based operating systems do not usually implement any type of ICMP rate limiting, so this scan operates very efficiently on Windows-based devices.

Disadvantage:

The UDP scan provides port information only. If additional version information is needed, the scan must be supplemented with a version detection scan (-sV) or the operating system fingerprinting option (-O).

The UDP scan requires privileged access, so this scan option is only available on systems with the appropriate user permissions.

Most networks have huge amounts of TCP traffic; as a result, the efficiency of the UDP scan is lost. The UDP scan will locate these open ports and provide the security manager with valuable information that can be used to identify these invasions achieved by the attacker on open UDP ports caused by spyware applications, Trojan horses, and other malicious software.



FIGURE 3.35: UDP Scanning

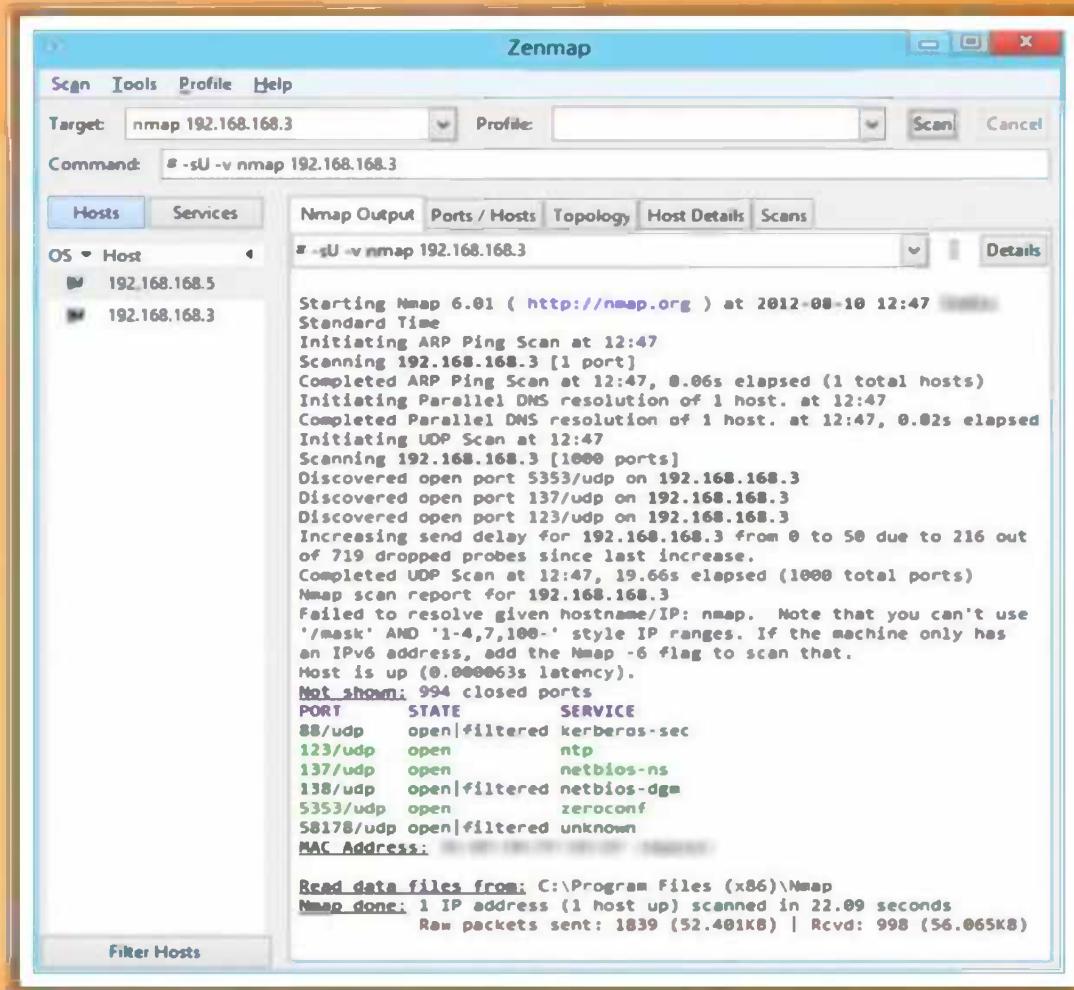
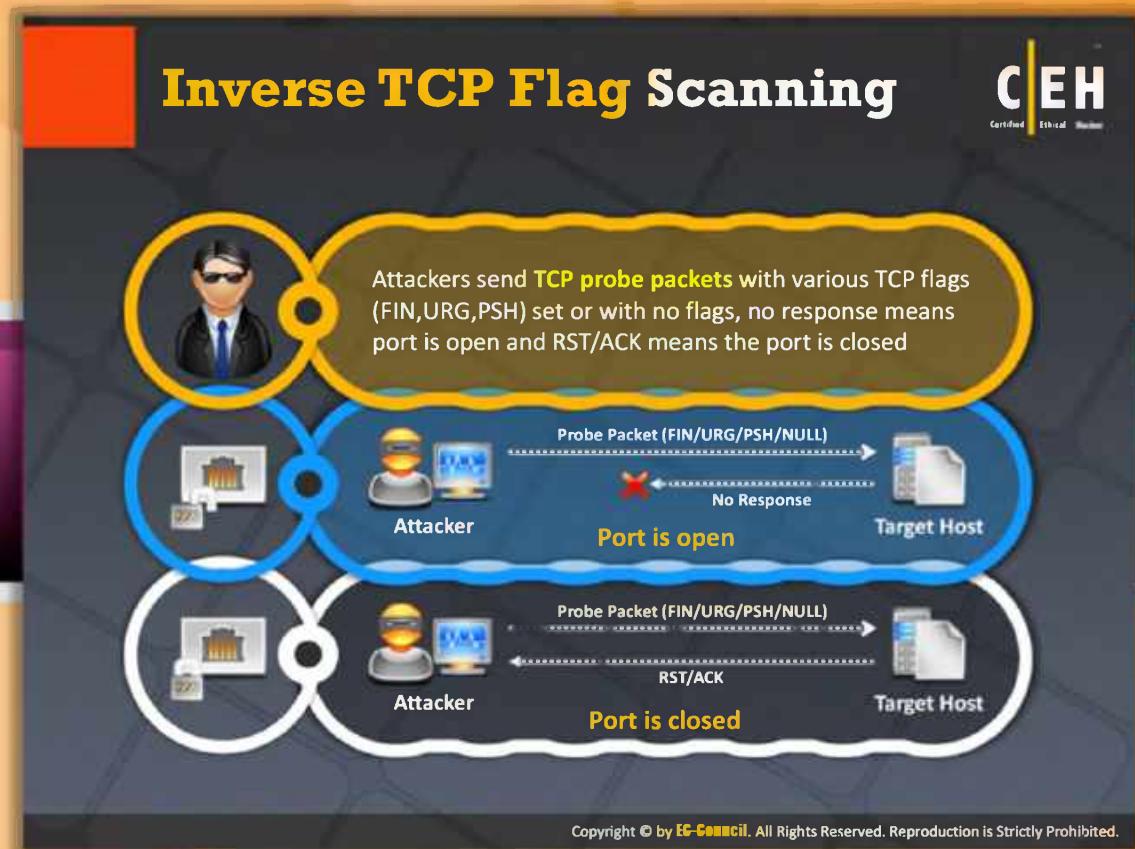


FIGURE 3.36: Zenmap showing UDP Scanning Result



Inverse TCP Flag Scanning

Attackers send the **TCP probe packets** by enabling various TCP flag (FIN, URG, PSH) or with no flags. When the port is open, the attacker doesn't get any response from the host, whereas when the port is closed, he or she receives the **RST/ACK** from the target host.

The SYN packets that are sent to the sensitive ports of the targeted hosts are detected by using security mechanisms such as **firewalls** and **IDS**. Programs such as Synlogger and Courtney are available to log half-open SYN flag scan attempts. At times, the probe packets enabled with TCP flags can pass through filters undetected, depending on the security mechanisms installed.

Probing a target using a half-open SYN flag is known as an inverted technique. It is called this because the closed ports can only send the response back. According to RFC 793, An RST/ACK packet must be sent for connection reset, when the port is closed on host side. Attackers take advantage of this feature to send TCP probe packets to each port of the target host with various TCP flags set.

Common flag configurations used for probe packet include:

- ⌚ A FIN probe with the FIN TCP flag set
- ⌚ An XMAS probe with the FIN, URG, and PUSH TCP flags set
- ⌚ A NULL probe with no TCP flags set

- ⌚ A SYN/ACK probe

All the closed ports on the targeted host will send an RST/ACK response. Since the RFC 793 standard is completely ignored in the operating system such as Windows, you cannot see the RST/ACK response when connected to the closed port on the target host. This technique is effective when used with UNIX-based operating systems.

Advantages

- ⌚ Avoids many IDS and logging systems, highly stealthy

Disadvantages

- ⌚ Needs raw access to network sockets, thus requiring super-user privileges
- ⌚ Mostly effective against hosts using a BSD-derived TCP/IP stack (not effective against Microsoft Windows hosts in particular)



FIGURE 3.37: Inverse TCP Flag Scanning when Port is Open



FIGURE 3.38: Inverse TCP Flag Scanning when Port is Closed

ACK Flag Scanning

A stealthy technique is used for **identifying open TCP ports**. In this technique a TCP packet with ACK flag ON is sent to the remote host and then the header information of the RST packets sent by remote host are analyzed. Using this technique one can exploit the potential vulnerabilities of BSD derived TCP/IP stack. This technique gives good results when used with certain operating systems and platforms.

ACK scanning can be performed in two ways:

- ⌚ TTL field analysis
 - ⌚ WINDOW field analysis

Using TTL value one can determine the number of systems the TCP packet traverses. You can send an ACK probe packet with random sequence number: no response means port is filtered (state full firewall is present) and RST response means the port is not filtered.

```
nmap -sA -P0 10.10.0.25
```

Starting nmap 5.21 (http://nmap.org) at 2010-05-16 12:15 EST

All 529 scanned ports on 10.10.0.25 are: filtered



FIGURE 3.39: ACK Flag Scanning when Stateful Firewall is Present



FIGURE 3.40: ACK Flag Scanning when No Firewall is Present

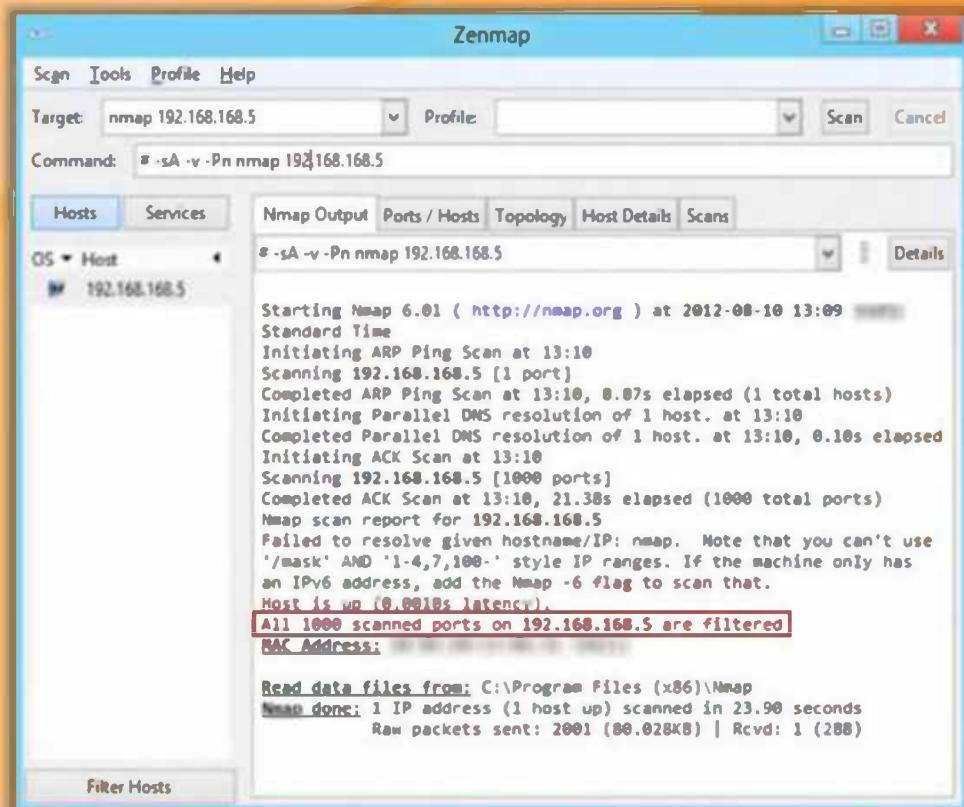


FIGURE 3.41: Zenmap showing ACK Flag Scanning Result



Scanning Tool: NetScan Tools Pro

Source: <http://www.netscantools.com>

NetScan Tools Pro is an **investigation tool**. It allows you to troubleshoot, monitor, discover, and detect devices on your network. You can **gather information** about the local LAN as well as Internet users, IP addresses, ports, etc. using this tool. You can find vulnerabilities and exposed ports in your system. It is the combination of many **network tools** and **utilities**. The tools are categorized by functions such as active, passive, DNS, and local computer.

Active Discovery and Diagnostic Tools: Used for testing and locating devices that are connected to your network.

Passive Discovery Tools: Monitors the activities of the devices that are connected to your network and also gathers information from third parties.

DNS Tools: Used to detect problems with DNS.

Local Computer and General Information Tools: Provides details about your local computer's network.

Benefits:

- The information gathering process is made simpler and faster by automating the use of many network tools

- Produces the result reports in your web browser clearly

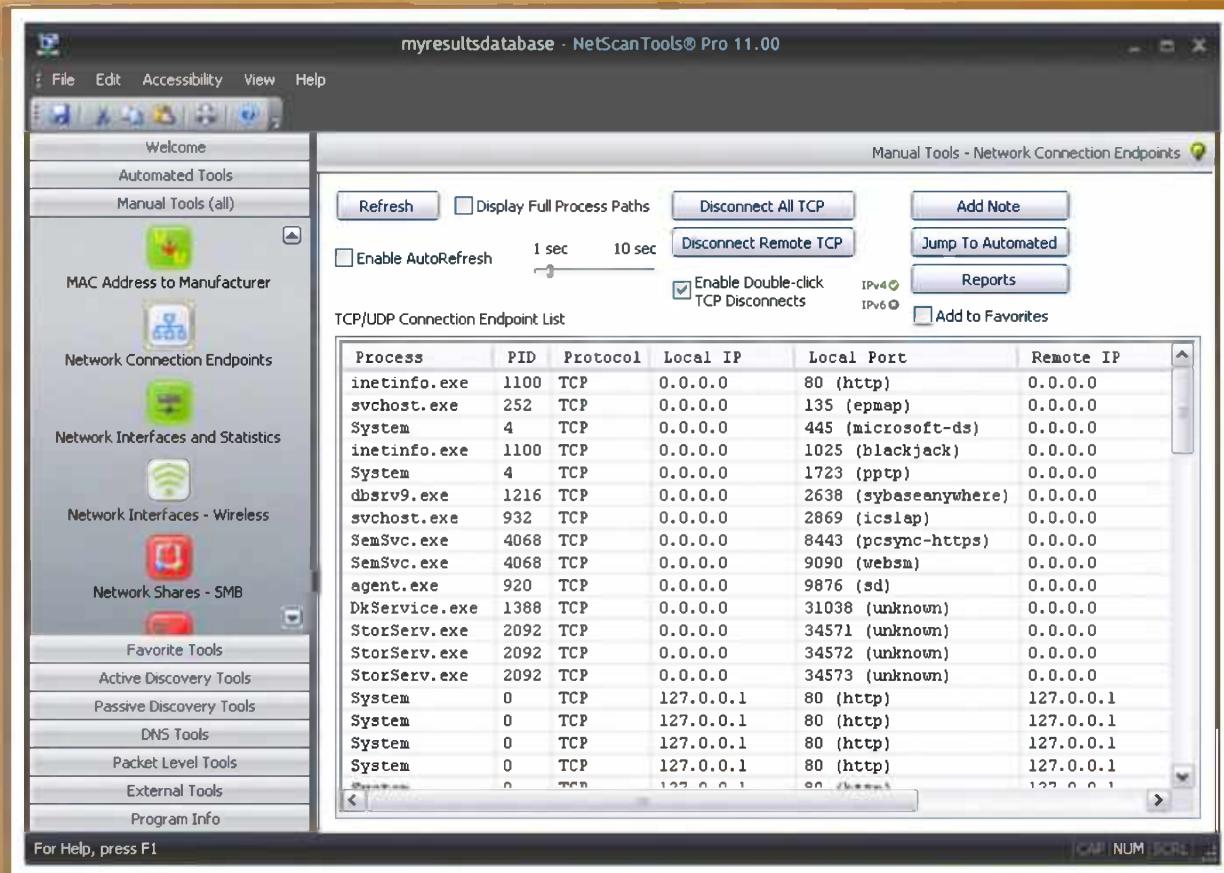


FIGURE 3.42: NetScan Tools Pro Screenshot

Scanning Tools

C|EH
Certified Ethical Hacker

 PRTG Network Monitor http://www.paessler.com	 Global Network Inventory Scanner http://www.magnetosoft.com
 Net Tools http://mabsoft.com	 SoftPerfect Network Scanner http://www.softperfect.com
 IP Tools http://www.ks-soft.net	 Advanced Port Scanner http://www.radmin.com
 MegaPing http://www.magnetosoft.com	 Netifera http://netifera.com
 Network Inventory Explorer http://www.10-strike.com	 Free Port Scanner http://www.nsauditor.com

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

Scanning Tools

Scanning tools ping computers, scan for listening **TCP/UDP ports**, and display the type of resources shared on the network (including system and hidden). The attacker may attempt to launch attacks against your network or network resources based on the information gathered with the help of scanning tools. A few of the scanning tools that can detect active ports on the systems are listed as follows:

- ⌚ PRTG Network Monitor available at <http://www.paessler.com>
- ⌚ Net Tools available at <http://mabsoft.com>
- ⌚ IP Tools available at <http://www.ks-soft.net>
- ⌚ MegaPing available at <http://www.magnetosoft.com>
- ⌚ Network Inventory Explorer available at <http://www.10-strike.com>
- ⌚ Global Network Inventory Scanner available at <http://www.magnetosoft.com>
- ⌚ SoftPerfect Network Scanner available at <http://www.softperfect.com>
- ⌚ Advanced Port Scanner available at <http://www.radmin.com>
- ⌚ Netifera available at <http://netifera.com>
- ⌚ Free Port Scanner available at <http://www.nsauditor.com>

Do Not Scan These IP Addresses (Unless you want to get into trouble)



<p>RANGE 128</p> <p>128.37.0.0 Army Yuma Proving Ground 128.38.0.0 Naval Surface Warfare Center 128.43.0.0 Defence Research Establishment-Ottawa 128.47.0.0 Army Communications Electronics Command 128.49.0.0 Naval Ocean Systems Center 128.50.0.0 Department of Defense 128.51.0.0 Department of Defense 128.56.0.0 U.S. Naval Academy 128.60.0.0 Naval Research Laboratory 128.63.0.0 Army Ballistics Research Laboratory 128.80.0.0 Army Communications Electronics Command 128.102.0.0 NASA Ames Research Center 128.149.0.0 NASA Headquarters 128.154.0.0 NASA Wallops Flight Facility 128.155.0.0 NASA Langley Research Center 128.156.0.0 NASA Lewis Network Control Center 128.157.0.0 NASA Johnson Space Center 128.158.0.0 NASA Ames Research Center 128.159.0.0 NASA Ames Research Center 128.160.0.0 Naval Research Laboratory 128.161.0.0 NASA Ames Research Center 128.183.0.0 NASA Goddard Space Flight Center 128.202.0.0 50th Space Wing 128.216.0.0 MacDill Air Force Base 128.217.0.0 NASA Kennedy Space Center 128.236.0.0 U.S. Air Force Academy</p> <p>RANGE 129</p> <p>129.23.0.0 Strategic Defense Initiative Organization 129.29.0.0 United States Military Academy 129.50.0.0 NASA Marshall Space Flight Center 129.51.0.0 Patrick Air Force Base 129.52.0.0 Wright-Patterson Air Force Base</p>	<p>129.53.0.0 - 129.53.255.255 66SPTG-SCB 129.54.0.0 Vandenberg Air Force Base, CA 129.92.0.0 Air Force Institute of Technology 129.99.0.0 NASA Ames Research Center 129.131.0.0 Naval Weapons Center 129.163.0.0 NASA/Johnson Space Center 129.164.0.0 NASA IV/V 129.165.0.0 NASA Goddard Space Flight Center 129.167.0.0 NASA Marshall Space Flight Center 129.168.0.0 NASA Lewis Research Center 129.190.0.0 Naval Underwater Systems Center 129.198.0.0 Air Force Flight Test Center 129.209.0.0 Army Ballistics Research Laboratory 129.229.0.0 U.S. Army Corps of Engineers 129.251.0.0 United States Air Force Academy</p> <p>RANGE 130</p> <p>130.40.0.0 NASA Johnson Space Center 130.90.0.0 Mather Air Force Base 130.109.0.0 Naval Coastal Systems Center 130.124.0.0 Honeywell Defense Systems Group 130.165.0.0 U.S. Army Corps of Engineers 130.167.0.0 NASA Headquarters</p> <p>RANGE 131</p> <p>131.6.0.0 Langley Air Force Base 131.10.0.0 Barksdale Air Force Base 131.17.0.0 Sheppard Air Force Base 131.21.0.0 Hahn Air Base 31.32.0.0 37 Communications Squadron 131.35.0.0 Fairchild Air Force Base 131.36.0.0 Yokota Air Base 131.37.0.0 Elmendorf Air Force Base 131.38.0.0 Hickam Air Force Base 131.39.0.0 354CS/SCSN</p>	<p>RANGE 132</p> <p>132.3.0.0 Williams Air Force Base 132.5.0.0 - 132.5.255.255 49th Fighter Wing 132.6.0.0 Ankara Air Station 132.7.0.0 - 132.7.255.255 SSG/SINO 132.9.0.0 28th Bomb Wing 132.10.0.0 319 Comm Sq 132.11.0.0 Hellenikon Air Base 132.12.0.0 Myrtle Beach Air Force Base 132.13.0.0 Bentwaters Royal Air Force Base 132.14.0.0 Air Force Concentrator Network 132.15.0.0 Kadena Air Base 132.16.0.0 Kunsan Air Base 132.17.0.0 Lindsey Air Station 132.18.0.0 McGuire Air Force Base 132.19.0.0 100CS (NET-MILDENHALL) 132.20.0.0 35th Communications Squadron 132.21.0.0 Pittsburgh Air Force Base 132.22.0.0 23Communications Sq 132.24.0.0 Dover Air Force Base 132.25.0.0 786 C/S/SCBBN 132.27.0.0 - 132.27.255.255 39CS/SCBBN 132.28.0.0 14TH COMMUNICATION SQUADRON 132.30.0.0 Lajes Air Force Base 132.31.0.0 Long Bldg Air Force Base 132.33.0.0 60CS/SCSNM 132.34.0.0 Cannon Air Force Base 132.35.0.0 Altus Air Force Base 132.37.0.0 75 ABW 132.38.0.0 Goodfellow AFB 132.39.0.0 K.I. Sawyer Air Force Base</p> <p>For a complete list, see the file in DVD IP ADDRESSES YOU SHOULD NOT SCAN.txt</p>
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

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

Do Not Scan These IP Addresses (Unless you want to get into trouble)

The IP addresses listed in the following table are associated with the critical information resource centers of the US. Scanning these IP addresses will be considered an attempt to break the US's information security. Therefore, do not scan these IP addresses unless you want to get into trouble.

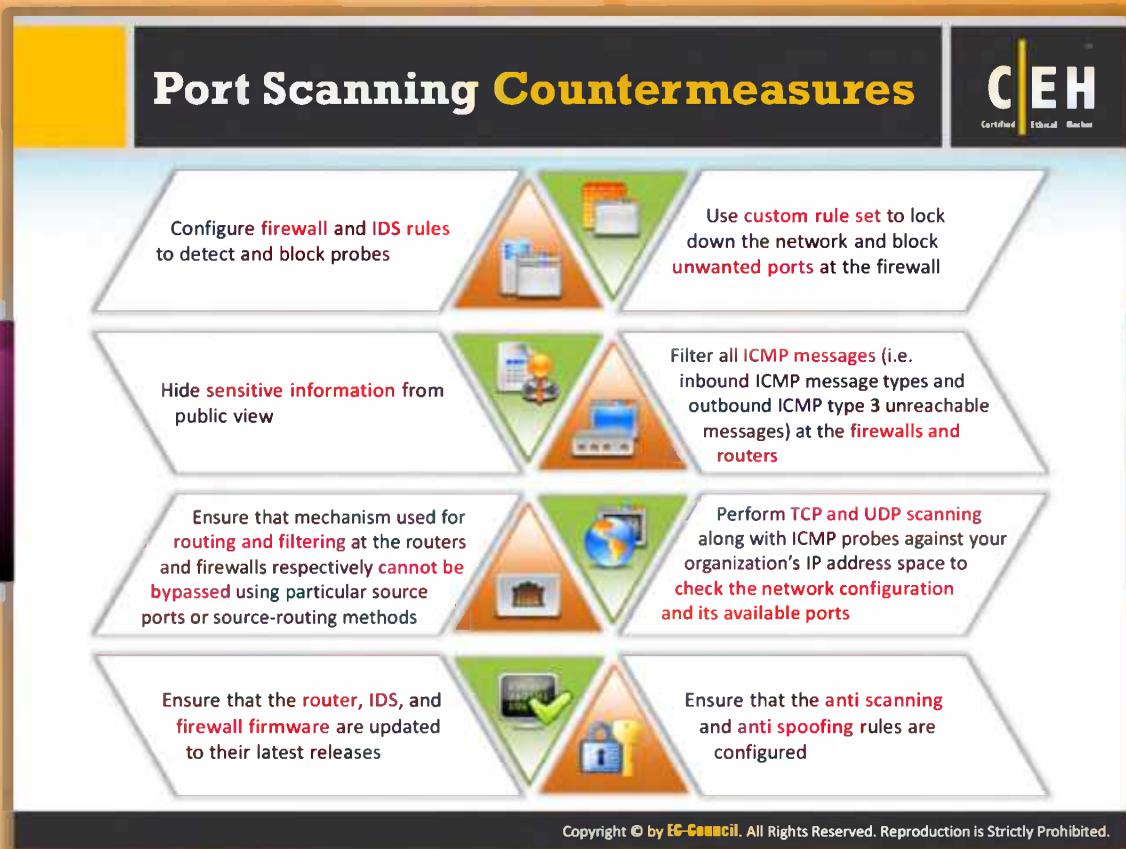
RANGE 6	129.51.0.0 Patrick Air Force Base
6.* – Army Information Systems Center	129.52.0.0 Wright-Patterson Air Force Base
RANGE 7	129.53.0.0 - 129.53.255.255 66SPTG-SCB
7.*.*.* Defense Information Systems Agency, VA	129.54.0.0 Vandenberg Air Force Base, CA
RANGE 11	129.92.0.0 Air Force Institute of Technology

11.*.*.* DoD Intel Information Systems, Defense Intelligence Agency, Washington DC	129.99.0.0 NASA Ames Research Center
RANGE 21	129.131.0.0 Naval Weapons Center
21. – US Defense Information Systems Agency	129.163.0.0 NASA/Johnson Space Center
RANGE 22	129.164.0.0 NASA IVV
22.* – Defense Information Systems Agency	129.165.0.0 NASA Goddard Space Flight Center
RANGE 24	129.167.0.0 NASA Marshall Space Flight Center
24.198.*.*	129.168.0.0 NASA Lewis Research Center
RANGE 25	129.190.0.0 Naval Underwater Systems Center
25.*.*.* Royal Signals and Radar Establishment, UK	129.198.0.0 Air Force Flight Test Center
RANGE 26	129.209.0.0 Army Ballistics Research Laboratory
26.* – Defense Information Systems Agency	129.229.0.0 U.S. Army Corps of Engineers
RANGE 29	129.251.0.0 United States Air Force Academy
29.* – Defense Information Systems Agency	RANGE 130
RANGE 30	130.40.0.0 NASA Johnson Space Center
30.* – Defense Information Systems Agency	130.90.0.0 Mather Air Force Base
RANGE 49	130.109.0.0 Naval Coastal Systems Center
49.* – Joint Tactical Command	130.124.0.0 Honeywell Defense Systems Group
RANGE 50	130.165.0.0 U.S.Army Corps of Engineers
50.* – Joint Tactical Command	130.167.0.0 NASA Headquarters
RANGE 55	RANGE 131
55.* – Army National Guard Bureau	131.6.0.0 Langley Air Force Base
RANGE 55	131.10.0.0 Barksdale Air Force Base

55.* – Army National Guard Bureau	131.17.0.0 Sheppard Air Force Base
55.* – Army National Guard Bureau	131.17.0.0 Sheppard Air Force Base
RANGE 62	131.21.0.0 Hahn Air Base
62.0.0.1 – 62.30.255.255 Do not scan!	31.32.0.0 37 Communications Squadron
RANGE 64	131.35.0.0 Fairchild Air Force Base
64.70.*.* Do not scan	131.36.0.0 Yokota Air Base
64.224.* Do not Scan	131.37.0.0 Elmendorf Air Force Base
64.225.* Do not scan	131.38.0.0 Hickam Air Force Base
64.226.* Do not scan	131.39.0.0 354CS/SCSN
RANGE 128	RANGE 132
128.37.0.0 Army Yuma Proving Ground	132.3.0.0 Williams Air Force Base
128.38.0.0 Naval Surface Warfare Center	132.5.0.0 - 132.5.255.255 49th Fighter Wing
128.43.0.0 Defence Research Establishment-Ottawa	132.6.0.0 Ankara Air Station
128.47.0.0 Army Communications Electronics Command	132.7.0.0 - 132.7.255.255 SSG/SINO
128.49.0.0 Naval Ocean Systems Center	132.9.0.0 28th Bomb Wing
128.50.0.0 Department of Defense	132.10.0.0 319 Comm Sq
128.51.0.0 Department of Defense	132.11.0.0 Hellenikon Air Base
128.56.0.0 U.S. Naval Academy	132.12.0.0 Myrtle Beach Air Force Base
128.60.0.0 Naval Research Laboratory	132.13.0.0 Bentwaters Royal Air Force Base
128.63.0.0 Army Ballistics Research Laboratory	132.14.0.0 Air Force Concentrator Network
128.80.0.0 Army Communications Electronics Command	132.15.0.0 Kadena Air Base
128.102.0.0 NASA Ames Research Center	132.16.0.0 Kunsan Air Base
128.149.0.0 NASA Headquarters	132.17.0.0 Lindsey Air Station
128.154.0.0 NASA Wallops Flight Facility	132.18.0.0 McGuire Air Force Base
128.155.0.0 NASA Langley Research Center	132.19.0.0 100CS (NET-MILDENHALL)

128.156.0.0 NASA Lewis Network Control Center	132.20.0.0 35th Communications Squadron
128.157.0.0 NASA Johnson Space Center	132.21.0.0 Plattsburgh Air Force Base
128.157.0.0 NASA Johnson Space Center	132.21.0.0 Plattsburgh Air Force Base
128.158.0.0 NASA Ames Research Center	132.22.0.0 23Communications Sq
128.159.0.0 NASA Ames Research Center	132.24.0.0 Dover Air Force Base
128.160.0.0 Naval Research Laboratory	132.25.0.0 786 CS/SCBM
128.161.0.0 NASA Ames Research Center	132.27.0.0 - 132.27.255.255 39CS/SCBBN
128.183.0.0 NASA Goddard Space Flight Center	132.28.0.0 14TH COMMUNICATION SQUADRON
128.202.0.0 50th Space Wing	132.30.0.0 Lajes Air Force Base
128.216.0.0 MacDill Air Force Base	132.31.0.0 Loring Air Force Base
128.217.0.0 NASA Kennedy Space Center	132.33.0.0 60CS/SCSNM
128.236.0.0 U.S. Air Force Academy	132.34.0.0 Cannon Air Force Base
RANGE 129	132.35.0.0 Altus Air Force Base
129.23.0.0 Strategic Defense Initiative Organization	132.37.0.0 75 ABW
129.29.0.0 United States Military Academy	132.38.0.0 Goodfellow AFB
129.50.0.0 NASA Marshall Space Flight Center	132.39.0.0 K.I. Sawyer Air Force Base

TABLE 3.3: Do Not Scan These IP Addresses Table

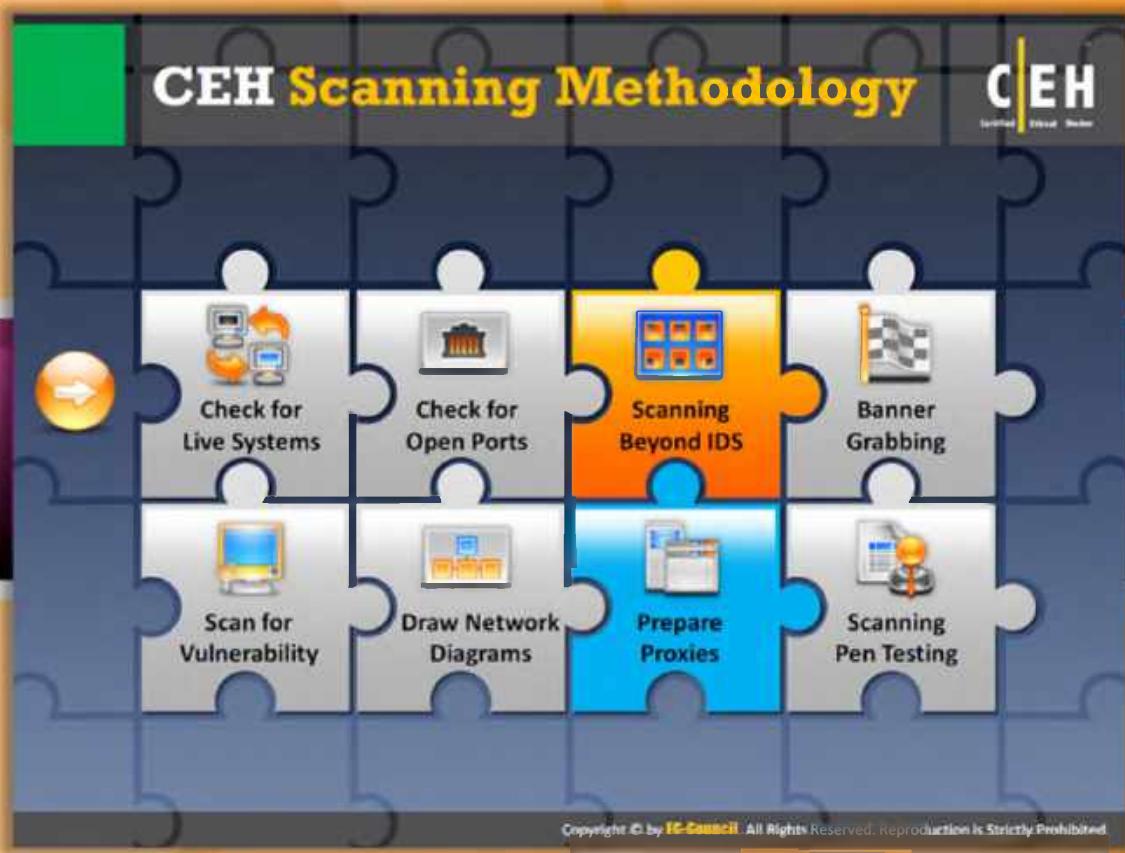


Port Scanning Countermeasures

As discussed previously, port scanning provides a lot of useful information such as IP addresses, host names, open ports, etc. to the attacker. Open ports especially provide an easy means for the attacker to **break into the security**. But there is nothing to worry about, as you can secure your system or network against port scanning by applying the following countermeasures:

- The firewall should be good enough to **detect probes** an attacker sends to scan the network. So the firewall should carry out stateful inspection if it has a specific rule set. Some firewalls do a better job than others in detecting stealth scans. Many firewalls have specific options to detect **SYN scans**, while others completely ignore FIN scans.
- Network intrusion detection systems should detect the OS detection method used by tools such as Nmap, etc. Snort (<http://snort.org>) is an intrusion detection and prevention technology that can be of great help, mainly because signatures are frequently available from public authors.
- Only necessary ports should be kept open; the rest of the ports should be filtered as the intruder will try to enter through any open port. This can be accomplished with the custom rule set. Filter inbound ICMP message types and all outbound ICMP type 3 unreachable messages at border routers and firewalls.

- ❸ Ensure that routing and filtering mechanisms cannot be bypassed using specific source ports or source-routing techniques.
- ❹ Test your own IP address space using TCP and UDP port scans as well as ICMP Probes to determine the network configuration and accessible ports.
- ❺ If a commercial firewall is in use, then ensure that the firewall is patched with the latest updates, antispoofing rules have been correctly defined, and fastmode services are not used in Check Point Firewall-1 environments.

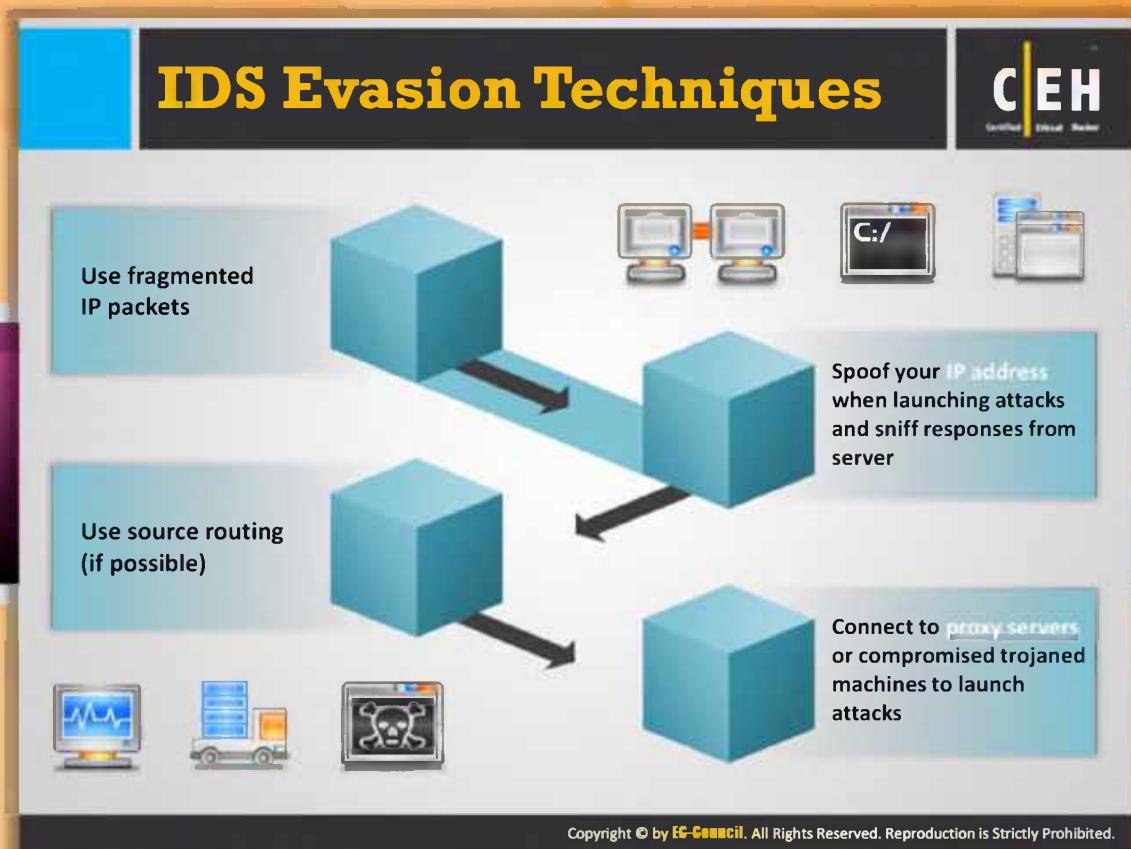


CEH Scanning Methodology

So far we have discussed how to check for live systems and open ports, the two common network vulnerabilities. An IDS is the security mechanism intended to prevent an attacker from entering a secure network. But, even the IDS has some limitations in offering security. Attackers are trying to launch attacks by exploiting limitations of IDS.

 Check for Live Systems	 Scan for Vulnerability
 Check for Open Ports	 Draw Network Diagrams
 Scanning Beyond IDS	 Prepare Proxies
 Banner Grabbing	 Scanning Pen Testing

This section highlights **IDS evasion techniques** and **SYN/FIN scanning**.



IDS Evasion Techniques

Most of the IDS evasion techniques rely on the use of fragmented probe packets that reassemble once they reach the target host. IDS evasion can also occur with the use of **spoofed fake hosts launching** network scanning probes.

Use fragmented IP packets

Attackers use different fragmentation methods to evade the IDS. These attacks are similar to session splicing. With the help of `fragroute`, all the probe packets flowing from your host or network can be fragmented. It can also be done with the help of a port scanner with fragmentation feature such as Nmap. This is accomplished because most IDS sensors fail to process large volumes of **fragmented packets**, as this involves greater CPU consumption and memory at the network sensor level.

Use source routing (if possible)

Source routing is a technique whereby the sender of a packet can specify the route that a packet should take through the network. It is assumed that the source of the packet knows about the layout of the network and can specify the best path for the packet.

SYN/FIN Scanning Using IP Fragments

The TCP header is split up into several packets so that the packet filters are not able to detect what the packets intend to do

It is not a new scanning method but a **modification** of the earlier methods

Command Prompt

```
C:\>nmap -sS -T4 -A -f -v 192.168.168.5
Starting Nmap 6.01 ( http://nmap.org ) at
2012-08-11 11:03 EDT
Initiating SYN Stealth Scan at 11:03
Scanning 192.168.168.5 [1000 ports]
Discovered open port 139/tcp on 192.168.168.5
Discovered open port 445/tcp on 192.168.168.5
Discovered open port 135/tcp on 192.168.168.5
Discovered open port 912/tcp on 192.168.168.5
Completed SYN Stealth Scan at 11:03, 4.75s
elapsed (1000 total ports)
```

SYN/FIN Scanning

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



SYN/FIN Scanning Using IP Fragments

SYN/FIN scanning using **IP fragments** is a modification of the earlier methods of scanning; the **probe packets** are further fragmented. This method came into existence to avoid the **false positive** from other scans, due to a packet filtering device present on the target machine. You have to split the **TCP header** into **several packets** instead of just sending a probe packet for avoiding the packet filters. Every TCP header should include the source and destination port for the first packet during any transmission: **(8 octet, 64 bit)**, and the initialized flags in the next, which allow the remote host to reassemble the packet upon receipt through an Internet protocol module that recognizes the fragmented data packets with the help of field equivalent values of protocol, source, destination, and identification.

Fragmented Packets

The TCP header, after splitting into small fragments, is transmitted over the network. But, at times you may observe unpredictable results such as fragmentation of the data in the IP header after the reassembly of IP on the server side. Some hosts may not be capable of parsing and reassembling the fragmented packets, and thus may cause crashes, reboots, or even network device monitoring dumps.

Firewalls

Some firewalls may have rule sets that block IP fragmentation queues in the kernel (like the CONFIG_IP_ALWAYS_DEFRAG option in the Linux kernel), although this is not widely implemented due to the adverse effect on performance. Since several intrusions detection systems employ signature-based methods to indicate scanning attempts based on IP and/or the TCP headers, fragmentation is often able to evade this type of packet filtering and detection. There is a probability of network problems on the target network.

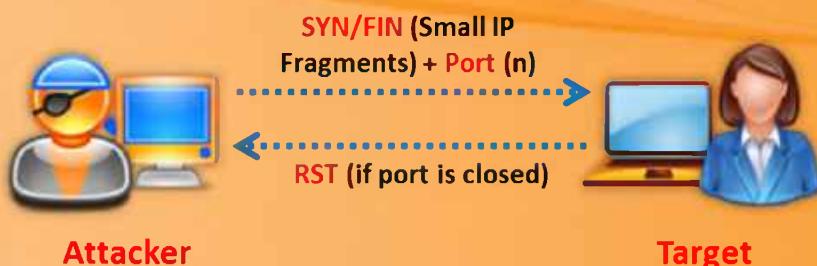
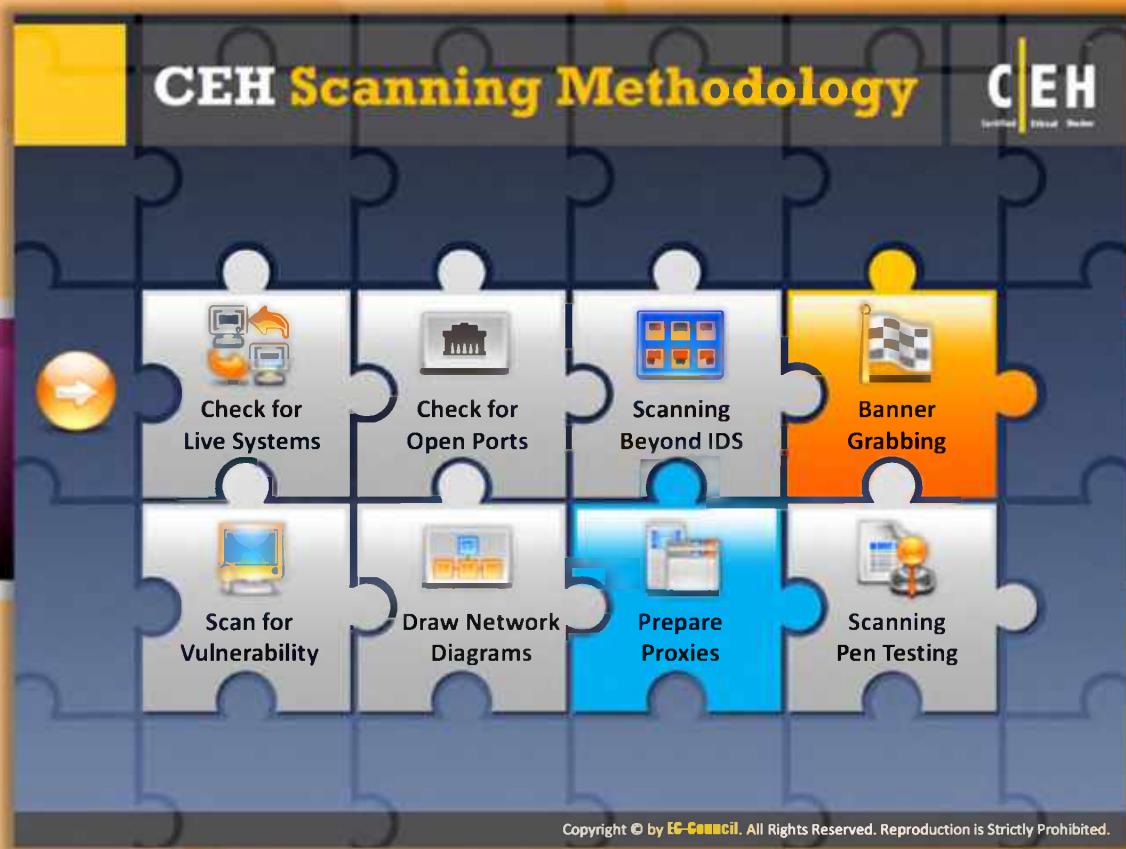


FIGURE 3.43: SYN/FIN Scanning

Nmap command prompts for SYN/FIN scan.

```
C:\>nmap -sS -T4 -A -f -v 192.168.168.5
Starting Nmap 6.01 ( http://nmap.org ) at 2012-08-11 11:03 EDT
Initiating SYN Stealth Scan at 11:03
Scanning 192.168.168.5 [1000 ports]
Discovered open port 139/tcp on 192.168.168.5
Discovered open port 445/tcp on 192.168.168.5
Discovered open port 135/tcp on 192.168.168.5
Discovered open port 912/tcp on 192.168.168.5
Completed SYN Stealth Scan at 11:03, 4.75s
elapsed (1000 total ports)
```

FIGURE 3.44: Nmap showing SYN/FIN Scanning Result



CEH Scanning Methodology

So far we have discussed how to check for live systems, open ports, and scan beyond IDS. All of these are the doorways for an attacker to break into a network. Another important tool of an attacker is banner grabbing, which we will discuss next.

 Check for Live Systems	 Scan for Vulnerability
 Check for Open Ports	 Draw Network Diagrams
 Scanning Beyond IDS	 Prepare Proxies
 Banner Grabbing	 Scanning Pen Testing

This section highlights banner grabbing, the need to perform banner grabbing, various ways of banner grabbing, and the tools that help in banner grabbing.

Banner Grabbing

C|EH Certified Ethical Hacker

■ Banner grabbing or OS fingerprinting is the method to determine the **operating system running on a remote target system**. There are two types of banner grabbing: active and passive.



Active Banner Grabbing

- Specially crafted packets are sent to remote OS and the response is noted
- The responses are then compared with a database to determine the OS
- Response from different OSes varies due to differences in TCP/IP stack implementation



Passive Banner Grabbing

- Banner grabbing from error messages: Error messages provide information such as type of server, type of OS, and SSL tool used by the target remote system
- Sniffing the network traffic: Capturing and analyzing packets from the target enables an attacker to determine OS used by the remote system
- Banner grabbing from page extensions: Looking for an extension in the URL may assist in determining the application version
Example: .aspx => IIS server and Windows platform

Why Banner Grabbing?

Identifying the OS used on the target host allows an attacker to **figure out the vulnerabilities the system posses** and the exploits that might work on a system to further **carry out additional attacks**



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



Banner Grabbing

Banner grabbing or OS fingerprinting is a method to determine the **operating system running on a remote target system**. Banner grabbing is important for hacking as it provides you with a greater probability of success in hacking. This is because most of the vulnerabilities are OS specific. Therefore, if you know the OS running on the target system, you can hack the system by exploiting the vulnerabilities specific to that operating system.

Banner grabbing can be carried out in two ways: either by spotting the banner while trying to connect to a service such as FTP or downloading the **binary file/bin/ls** to check the architecture with which it was built.

Banner grabbing is performed using the fingerprinting technique. A more advanced fingerprinting technique depends on stack querying, which transfers the packets to the network host and evaluates packets based on the reply. The first stack querying method was designed considering the TCP mode of communication, in which the response of the connection requests is evaluated. The next method was known as ISN (Initial Sequence Number) analysis. This identifies the differences in the random number generators found in the TCP stack. A new method, using the ICMP protocol, is known as **ICMP response analysis**. It consists of sending the ICMP messages to the remote host and evaluating the reply. The latest ICMP messaging is

known as temporal response analysis. Like others, this method uses the TCP protocol. Temporal response analysis looks at the **retransmission timeout (RTO)** responses from a remote host.

There are two types of banner grabbing techniques available; one is active and the other is passive.



Active Banner Grabbing

Active banner grabbing is based on the principle that an operating system's IP stack has a unique way of responding to specially crafted TCP packets. This arises because of different interpretations that vendors apply while implementing the TCP/IP stack on the particular OS. In active banner grabbing, a variety of malformed packets are sent to the remote host, and the responses are compared to a database.

For instance, in Nmap, the **OS fingerprint** or **banner grabbing** is done through eight tests. The eight tests are named T1, T2, T3, T4, T5, T6, T7, and PU (port unreachable). Each of these tests is illustrated as follows, as described in www.packetwatch.net:

T1: In this test, a TCP packet with the SYN and ECN-Echo flags enabled is sent to an open TCP port.

T2: It involves sending a TCP packet with no flags enabled to an open TCP port. This type of packet is known as a NULL packet.

T3: It involves sending a TCP packet with the URG, PSH, SYN, and FIN flags enabled to an open TCP port.

T4: It involves sending a TCP packet with the ACK flag enabled to an open TCP port.

T5: It involves sending a TCP packet with the SYN flag enabled to a closed TCP port.

T6: It involves sending a TCP packet with the ACK flag enabled to a closed TCP port.

T7: It involves sending a TCP packet with the URG, PSH, and FIN flags enabled to a closed TCP port.

PU (Port Unreachable): It involves sending a UDP packet to a closed UDP port. The objective is to extract an "**ICMP port unreachable**" message from the target machine.

The last test that Nmap performs is named TSeq for TCP Sequencability test. This test tries to determine the sequence generation patterns of the TCP initial sequence numbers, also known as **TCP ISN sampling**, the IP identification numbers (also known as **IPID sampling**), and the TCP timestamp numbers. The test is performed by sending six TCP packets with the SYN flag enabled to an open TCP port.

The objective is to find patterns in the initial sequence of numbers that the TCP implementations choose while responding to a connection request. These can be categorized into many groups such as the traditional **64K** (many old UNIX boxes), random increments (newer versions of Solaris, IRIX, FreeBSD, Digital UNIX, Cray, and many others), or True "random" (Linux 2.0.* , OpenVMS, newer AIX, etc.). Windows boxes use a "time-dependent" model where the ISN is incremented by a fixed amount for each time period.

Source: www.insecure.org, "Most operating systems increment a system-wide IPID value for each packet they send. Others, such as **OpenBSD**, use a random IPID and some systems (like Linux) use an IPID of 0 in many cases where the 'Don't Fragment' bit is not set. Windows does not put the IPID in network byte order, so it increments by **256** for each packet. Another number that can be sequenced for OS detection purposes is the TCP timestamp option values. Some systems do not support the feature; others increment the value at frequencies of 2HZ, 100HZ, or 1000HZ and still others return 0."



Passive Banner Grabbing

Source: <http://honeynet.org>

Like active banner grabbing, passive banner grabbing is also based on the differential implementation of the stack and the various ways an OS responds to packets. However, instead of relying on scanning the target host, passive fingerprinting captures packets from the target host via sniffing to study for telltale signs that can reveal an OS.

The four areas that are typically noted to determine the operating system are:

- ⌚ TTL - What the operating system sets the Time To Live on the outbound packet
- ⌚ Window Size - what the operating system sets the Window size
- ⌚ DF - Does the operating system set the Don't Fragment bit
- ⌚ OS - Does the operating system set the Type of Service, and if so, at what

Passive fingerprinting has to be neither fully accurate nor be limited to these four signatures. However, by looking at several signatures and combining information, accuracy can be improved. The following is the analysis of a sniffered packet dissected by Lance Spitzner in his paper on passive fingerprinting (<http://www.honeynet.org/papers/finger/>).

04/20-21:41:48.129662 129.142.224.3:659 -> 172.16.1.107:604

TCP TTL:45 TOS:0x0 ID:56257

***F**A* Seq: 0x9DD90553

Ack: 0xE3C65D7 Win: 0x7D78

Based on the four criteria, the following are identified:

- ⌚ TTL: 45
- ⌚ Window Size: 0x7D78 (or 32120 in decimal)
- ⌚ DF: The Don't Fragment bit is set
- ⌚ TOS: 0x0

Database Signatures

This information is then compared to a database of signatures. Considering the TTL used by the remote host, it is determined from the sniffer trace that the TTL is set at 45. This indicates that it went through **19 hops** to get to the target, so the original TTL must have been set at 64.

Based on this TTL, it appears that the packet was sent from a **Linux or FreeBSD** box (however, more system signatures need to be added to the database). This TTL is confirmed by doing a traceroute to the remote host. If the trace needs to be done stealthily, the traceroute time-to-live (**default 30 hops**) can be set to be one or two hops less than the remote host (-m option). Setting traceroute in this manner reveals the path information (including the upstream provider) without actually touching the remote host.

Window Sizes

The next step is to **compare window sizes**. The window size is another effective tool that determines specifically what window size is used and how often the size is changed. In the previous signature, it is set at **0x7D78**, a default window size is commonly used by Linux. In addition, FreeBSD and Solaris tend to maintain the same window size throughout a session. However, Cisco routers and Microsoft Windows/NT window sizes are constantly changing. The window size is more accurate if measured after the initial three-way handshake (due to TCP slow start).

Session Based

Most systems use the DF bit set, so this is of limited value. However, this does make it easier to identify the few systems that do not use the **DF flag** (such as **SCO or OpenBSD**). TOS is also of limited value, since it seems to be more session-based than **operating-system-based**. In other words, it is not so much the operating system that determines the TOS, but the protocol used. Therefore, based on this information, specifically TTL and window size, one can compare the results to the database of signatures and, with a degree of confidence, determine the OS (in this case, Linux kernel 2.2.x).

Just as with active fingerprinting, passive fingerprinting has some limitations. First, applications that build their own packets (such as Nmap, hunt, nemesis, etc.) will not use the same signatures as the operating system. Second, it is relatively simple for a remote host to adjust the TTL, window size, DF, or TOS setting on packets.

Passive fingerprinting can be used for several other purposes. Crackers can use “stealthy” fingerprinting. For example, to determine the operating system of a potential target, such as a web server, one need only request a web page from the server, and then analyze the sniffer traces. This bypasses the need for using an active tool that various IDS systems can detect. Also, passive fingerprinting may be used to identify remote proxy firewalls. Since proxy firewalls rebuild connections for clients, it may be possible to ID proxy firewalls based on the signatures that have been discussed. Organizations can use passive fingerprinting to identify rogue systems on their network. These would be systems that are not authorized on the network.



Why Banner Grabbing?

Identifying the OS used on the target host allows an attacker to figure out the vulnerabilities the system possesses and the exploits that might work on a system to further carry out additional attacks.

Banner Grabbing Tools

C|EH
Certified Ethical Hacker

- ID Serve is used to identify the **make, model, and version** of any web site's server software
- It is also used to **identify non-HTTP (non-web) Internet servers** such as FTP, SMTP, POP, NEWS, etc.

- Netcraft reports a site's **operating system, web server, and netblock owner** together with, if available, a graphical view of the time since last reboot for each of the computers serving the site

ID Serve



<http://www.grc.com>

Netcraft



<http://toolbar.netcraft.com>

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



Banner Grabbing Tools

Banner grabbing can be done even with the help of tools. Many tools are available in the market. These tools make banner grabbing an easy task. The following are examples of banner grabbing tools:



ID Serve

Source: <http://www.grc.com>

ID Serve is used to identify the make, model, and version of any website's server software; it is also used to identify non-HTTP (non-web) Internet servers such as FTP, SMTP, POP, NEWS, etc.

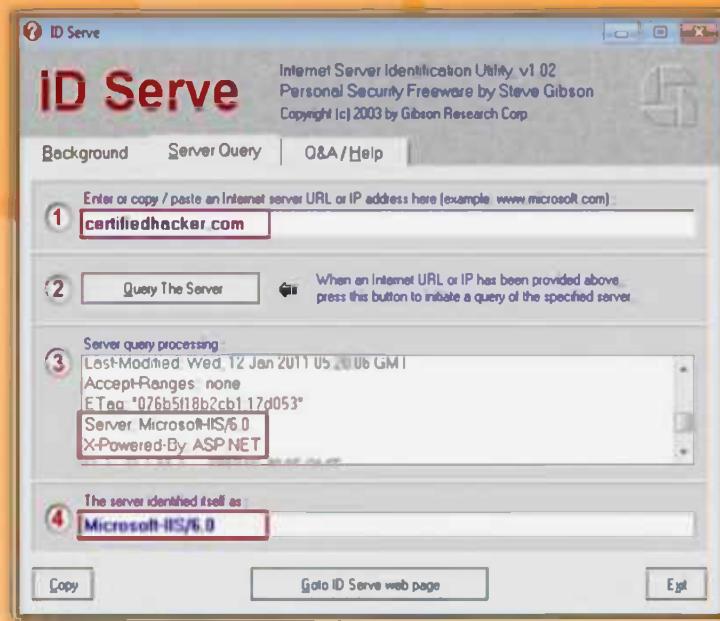


FIGURE 3.45: ID Serve Screenshot



Source: <http://toolbar.netcraft.com>

Netcraft reports a site's operating system, web server, and netblock owner together with, if available, a graphical view of the time since last reboot for each of the computers serving the site.

The screenshot shows the Netcraft Site report for 'certifiedhacker.com'. The main table provides detailed information about the site's infrastructure:

Site	http://certifiedhacker.com	Last reboot	1 day ago	Last Uptime graph
Domain	certifiedhacker.com	Netblock	TM VADS DC Hosting	graph
IP address	202.75.54.101	Site rank	270501	
Country	MY	Name server	ns0.noyearlyfees.com	
Date first seen	December 2002	DNS admin	admin@noyearlyfees.com	
Domain	tukows.com	Reverse DNS	ns1.noyearlyfees.com	
Registrar		Name server	Success Idea IT Services	
Organization	certifiedhacker.com, certifiedhacker.com, 92345, United States	Organization	Damansara Jaya, Petaling Jaya, Selangor, 47400, Malaysia	

Below the table, there is a 'Check another site:' input field and a 'Hosting History' section showing the netblock owner, IP address, OS, Web Server, and last changed date for multiple instances of the site.

FIGURE 3.46: Netcraft Screenshot

Banner Grabbing Tools (Cont'd)

Netcat

This utility reads and writes data across network connections, using the TCP/IP protocol

```
1. # nc -vv www.juggyboy.com 80 -press[Enter]
2. GET / HTTP/1.0 - Press [Enter] twice
```

Server Identified as Microsoft-IIS/6.0

Telnet

This technique probes HTTP servers to determine the Server field in the HTTP response header

```
1. telnet www.certifiedhacker.com 80 - press[Enter]
2. GET / HTTP/1.0 - Press [Enter] twice
```

Server Identified as Microsoft-IIS/6.0

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

Banner Grabbing Tools (Cont'd)



Netcat

Source: <http://netcat.sourceforge.net>

Netcat is a networking utility that **reads** and **writes data** across network connections, with the help of the TCP/IP protocol. It is designed to be a reliable "**back-end**" tool that can be used directly or easily driven by other programs and scripts. It provides access to the following key features:

- ⊖ Outbound and inbound connections, TCP or UDP, to or from any ports.
- ⊖ Featured tunneling mode, which also allows special tunneling such as UDP to TCP, with the possibility of specifying all network parameters (source port/interface, listening port/interface), and the remote host allowed to connect to the tunnel.
- ⊖ Built-in port-scanning capabilities, with randomizer.
- ⊖ Advanced usage options, such as buffered send-mode (one line every N seconds) and hexdump (to stderr or to a specified file) of transmitted and received data.

Optional RFC854 telnet codes parser and responder. You can use the Netcat tool for grabbing the banner of a website by following this process. Here, the banner grabbing is done on the www.Juggyboy.com web server for gathering the server fields such as server type, version, etc.

- ② # nc -vv www.juggyboy.com 80 - press[Enter]
- ③ GET / HTTP/1.0 - Press [Enter] twice

From the screenshot, you can observe the area highlighted in red color is a server version (Microsoft-IIS/6.0).

```
root@bt:~# nc -vv www.juggyboy.com 80
DNS fwd/rev mismatch: www.juggyboy.com != w2k3.web26.prod.netsolhost.com
www.juggyboy.com [205.178.152.26] 80 (www) open
GET / HTTP/1.0

HTTP/1.1 200 OK
Connection: close
Date: Mon, 13 Aug 2012 12:14:16 GMT
Content-Length: 2165
Content-Type: text/html
Content-Location: http://10.49.99.26/default.htm
Last-Modified: Wed, 19 Apr 2006 22:09:12 GMT
Accept-Ranges: none
ETag: "8b46be3fd63c61:7a49"
Server: Microsoft-IIS/6.0
MicrosoftOfficeWebServer: 5.0 Pub
X-Powered-By: ASP.NET
```

FIGURE 3.47: Netcat showing Banner Grabbing Result



Telnet

This technique probes **HTTP servers** to determine the Server field in the HTTP response header.

For instance, if you want to enumerate a host running http (tcp 80), then you have to follow this procedure:

- ④ First, open the command prompt window.
- Go to **Start** → **Run**, type **cmd**, and press **Enter** or click **OK**.
- ⑤ In the command prompt window, request telnet to connect to a host on a specific port: C:\telnet www.certifiedhacker.com 80 and press **Enter**.
- ⑥ Next, you will get a blank screen where you have to type **GET / HTTP/1.0** and press **Enter** twice.
- ⑦ In the final step, the http server responses with the server version, say Microsoft-IIS/6.0. From the screenshot you can see the area highlighted in red color is the server version details.

```
C:\Windows\system32\cmd.exe
HTTP/1.1 403 Forbidden
Content-Length: 218
Content-Type: text/html
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Date: Sat, 11 Aug 2012 09:57:07 GMT
Connection: close

<html><head><title>Error</title></head><body><head><title>Directory Listing Denied</title></head>
<body><h1>Directory Listing Denied</h1>This Virtual Directory does not allow contents to be listed.</body></body></html>

Connection to host lost.
```

FIGURE 3.48: Command Prompt showing http server responses with the server version

Banner Grabbing Countermeasures: Disabling or Changing Banner



-  Display false banners to misguide the attackers
-  Turn off unnecessary services on the network host to limit the information disclosure
-  IIS users can use these tools to disable or change banner information
 - IIS Lockdown Tool (<http://microsoft.com>)
 - ServerMask (<http://www.port80software.com>)
-  Apache 2.x with mod_headers module - use a directive in httpd.conf file to change banner information Header set Server "New Server Name"
-  Alternatively, change the ServerSignature line to ServerSignature Off in httpd.conf file

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



Banner Grabbing Countermeasures: Disabling or Changing Banners

Attackers use banner grabbing techniques and find out **sensitive information** such as device types, operating systems, application version, etc. used by the victim. With the help of the gathered information, the attacker exploits the vulnerabilities that are not updated with the **security patches** and launches the attacks. So, to protect your system against banner grabbing attacks, a few countermeasures can be adopted and they are listed as follows:

Disabling or Changing Banner

- Display false banners to misguide attackers
- Turn off unnecessary services on the network host to limit information disclosure
- IIS users can use these tools to disable or change banner information:
 - IIS Lockdown Tool (<http://microsoft.com>)
 - ServerMask (<http://www.port80software.com>)
- Apache 2.x with mod_headers module - use a directive in httpd.conf file to change banner information Header set Server "New Server Name"
- Alternatively, change the ServerSignature line to ServerSignature Off in the httpd.conf file

Hiding File Extensions from Web Pages

C|EH
Certified Ethical Hacker

The diagram features a central globe icon surrounded by five circular icons, each representing a different method to hide file extensions:

- IIS users use tools such as PageXchanger to manage the file extensions**: Represented by a purple circle containing a CD-ROM icon.
- Hide file extensions to mask the web technology**: Represented by an orange circle containing a document icon.
- Apache users can use mod_negotiation directives**: Represented by a blue circle containing a file icon.
- Change application mappings such as .asp with .htm or .foo, etc. to disguise the identity of the servers**: Represented by a green circle containing a folder icon.
- File extensions reveal information about the underlying server technology that an attacker can utilize to launch attacks**: Represented by a red circle containing a folder icon.

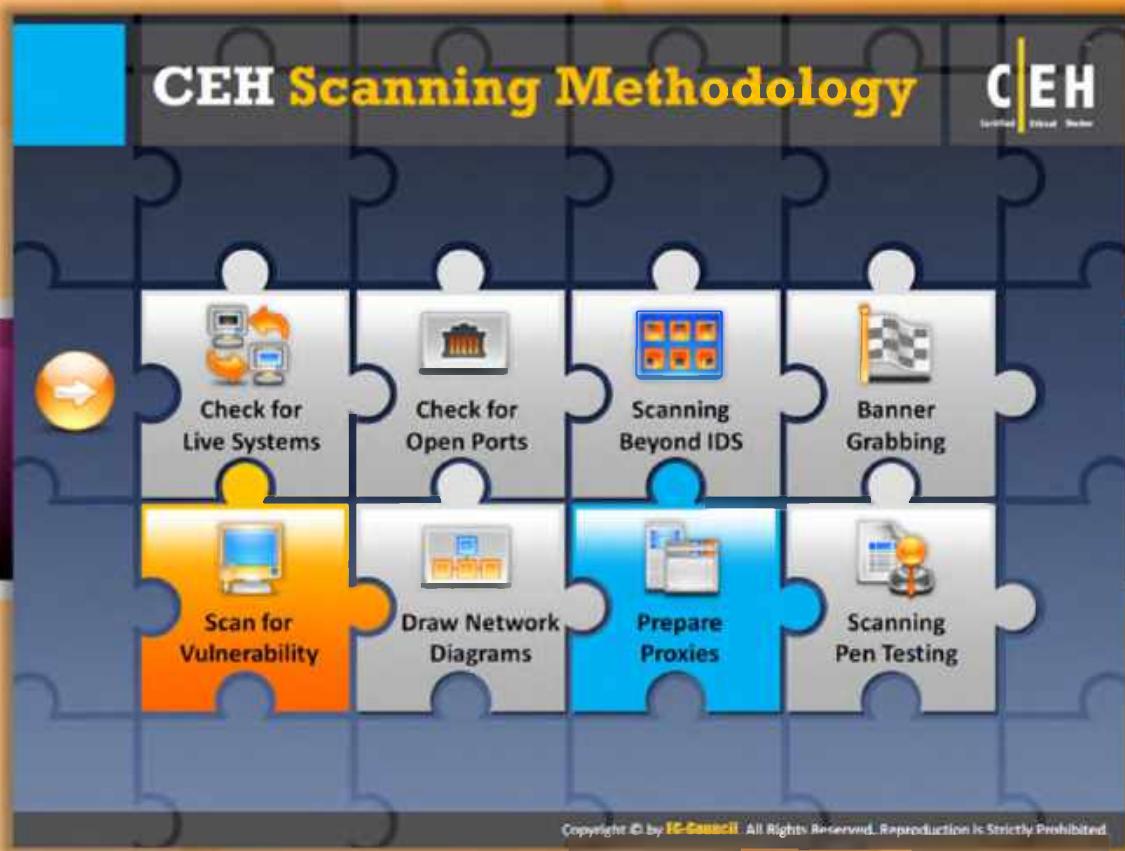
It is even better if the file extensions are not at all used

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



Hiding File Extensions from Web Pages

File extensions provide information about the **underlying server technology**; attackers can use this information to search vulnerabilities and launch attacks. Hiding file extensions is a good practice to mask **technology-generating** dynamic pages. Change application mappings such as .asp with .htm or .foo, etc. to disguise the identity of the servers. Apache users can use `mod_negotiation` directives. IIS users use tools such as **PageXchanger** to manage the file extensions. Doing without file extensions altogether is an even better idea.



CEH Scanning Methodology

So far, we have discussed how to check for live systems, open ports, scan beyond IDS, and the use of banner grabbing. All these concepts help an attacker or security administrator to find the loopholes that may allow an attacker into their network. Now we will discuss vulnerability scanning, a more detailed tests to determine vulnerabilities in a network, and its resources.

Check for Live Systems	Scan for Vulnerability
Check for Open Ports	Draw Network Diagrams
Scanning Beyond IDS	Prepare Proxies
Banner Grabbing	Scanning Pen Testing

This section describes vulnerability scanning and various vulnerability scanning tools.

Vulnerability Scanning

C|EH
Certified Ethical Hacker

Vulnerability scanning identifies **vulnerabilities** and **weaknesses** of a system and network in order to determine how a system can be exploited

The diagram features four overlapping diamond shapes arranged in a square pattern. The top-left diamond contains 'Network topology and OS vulnerabilities'. The top-right diamond contains 'Open ports and running services'. The bottom-left diamond contains 'Application and services vulnerabilities'. The bottom-right diamond contains 'Application and services configuration errors'. Each diamond has a small colored icon in its top-left corner: a blue square with four smaller squares inside, a grey square with a computer monitor icon, a grey square with a server icon, and a grey square with a battery icon respectively. There are also small icons of a computer monitor and a server tower on the left and right sides of the diamonds.

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



Vulnerability Scanning

Vulnerability scanning identifies **vulnerabilities** and **weaknesses** of a system and network in order to determine how a system can be exploited. Similar to other security tests such as **open port scanning** and **sniffing**, the vulnerability test also assists you in securing your network by determining the **loopholes** or vulnerabilities in your current security mechanism. This same concept can also be used by attackers in order to find the weak points of the target network. Once they find any weak points, they can exploit them and get in to the target network. Ethical hackers can use this concept to determine the security weaknesses of their target business and fix them before the bad guys find and exploit them.

Vulnerability scanning can find the vulnerabilities in:

- ⌚ Network topology and OS vulnerabilities
- ⌚ Open ports and running services
- ⌚ Application and services configuration errors
- ⌚ Application and services vulnerabilities

Vulnerability Scanning Tool: Nessus

Nessus is the vulnerability and configuration assessment product

Features

- Agentless auditing
- Compliance checks
- Content audits
- Customized reporting
- High-speed vulnerability discovery
- In-depth assessments
- Mobile device audits
- Patch management integration
- Scan policy design and execution

The screenshot shows a Nessus scan report titled "Report - Nessus Scan - 2012-08-20 10:45:00". It lists various vulnerabilities across different hosts, categorized by severity (Info, Low, Medium, High, Critical) and type (e.g., OS, Network, Application). Examples include "Windows Taskbar Information Disclosure", "Microsoft Windows SMB Registry - Nessus Correct Access the Webroot Registry", and "Microsoft Windows SP5400P Autostartable Process-Process-Network Listener".

<http://www.tenable.com>

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



Vulnerability Scanning Tool: Nessus

Source: <http://www.tenable.com>

Nessus is a **vulnerability scanner—a program** that searches for bugs in software. This tool allows a person to discover a specific way to violate the security of a software product. The vulnerability, in various levels of detail, is then disclosed to the user of the tool. The various steps this tool follows are:

- ⌚ Data gathering
- ⌚ Host identification
- ⌚ Port scan
- ⌚ Plug-in selection
- ⌚ Reporting of data

To obtain more accurate and detailed information from **Windows-based hosts** in a Windows domain, the user can create a domain group and account that have remote registry access privileges. After completing this task, he or she gets access not only to the registry key settings but also to the Service Pack patch levels, Internet Explorer vulnerabilities, and services running on the host.

It is a client-server application. The Nessus server runs on a UNIX system, keeps track of all the different vulnerability tests, and performs the actual scan. It has its own user database and secures authentication methods, so that remote users using the Nessus client can log in, configure a vulnerability scan, and send it on its way. Nessus includes **NASL (Nessus Attack Scripting Language)**, a language designed to write security tests.

The various features of Nessus are:

- Each security test is written as a **separate plug-in**. This way, the user can easily add tests without having to read the code of the Nessus engine.
- It performs smart service recognition. It assumes that the target hosts will respect the IANA assigned port numbers.
- The Nessus Security Scanner is made up of two parts: A server, which performs the attack, and a client, which is the front end. The server and the client can be run on different systems. That is, the user can audit his whole network from his personal computer, whereas the server performs its attacks from the main frame, which may be located in a different area.

The screenshot shows the Nessus web interface with the following details:

- Header:** Nessus logo, Reports, Mobile, Scans, Policies, Users, Configuration, Admin, Help, News, Log out.
- Breadcrumbs:** Scan LAN > Vulnerability Summary > Host Summary.
- Message:** Running - Launched Aug 13, 2012 18:07.
- Filters:** No Filters, Add Filter, Clear Filters.
- Table Headers:** Plugin ID, Count, Severity, Name, Family.
- Table Data:** A list of vulnerabilities with the following columns:
 - Plugin ID: 51192, 11714, 57606, 14272, 10736, 22964, 11219, 10167, 10663, 10111, 24260, 56644, 10147, 10150, 10194, 10295, 11422, 11956, 12053, 12654, 20108, 20301, 34242, 20117, 42010, 42111.
 - Count: 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1.
 - Severity: Medium, Medium, Medium, Info, Info.
 - Name: SSL Certificate Cannot Be Trusted, Remote Page (A) Physical Path Disclosure, SMB Signing Disabled, netcat portscanner (SSH), DCE Services Enumeration, Service Detection, Nessus SYN scanner, HTTP Server Type and Version, SSL Certificate Information, Microsoft Windows SMB Service Detection, HyperText Transfer Protocol (HTTP) Information, SSL / TLS Versions Supported, Nessus Server Detection, Windows NetBIOS / SMB Remote Host Information Disclosure, Microsoft Windows SMB Log In Possible, Microsoft Windows SMB NetLogonManager Remote System Information Disclosure, Web Server Unconfigured - Default Install Page Present, OS Identification, Host Fully Qualified Domain Name (FQDN) Resolution, Authenticated Check: OS Name and Installed Package Enumeration, Web Server / Application Identifier Vendor Fingerprinting, VMware ESX/ESXi Server detection, Microsoft .NET Handlers Enumeration, Microsoft Windows SMB Registry : Nessus Cannot Access The Windows Registry, Microsoft Windows NTLMSESP Authentication Request Remote Network Name Disclosure, HTTP Methods Allowed (per directory).
 - Family: General, Web Servers, Mac, Port scanners, Windows, Service detection, Port scanners, Web Servers, General, Windows, Web Servers, General, Service detection, Windows, Windows, Windows, Web Servers, General, General, Settings, Web Servers, Service detection, Web Servers, Windows, Windows, Web Servers.

FIGURE 3.49: Nessus Screenshot

The screenshot shows the GFI LanGuard 2012 software interface. At the top, there's a navigation bar with tabs like Dashboard, Scan, Remediate, Audit Monitor, Reports, Configuration, Options, and Help. Below the navigation bar is a main dashboard area. On the left, there's a sidebar with sections for Filter, Group, Overview, Computer, Network, Vulnerabilities, Patches, Ports, Software, Hardware, and System Information. The central part of the screen displays various metrics and charts. One chart shows 'Computer Health Trending' with a red line graph. Another section shows 'Computer Vulnerability Distribution' with a pie chart. The bottom of the interface has a footer with links for Support, GFI Software, News & Events, and Contact Us, along with a copyright notice: 'Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.'



Vulnerability Scanning Tool: GFI LanGuard

Source: <http://www.gfi.com>

GFI LanGuard acts as a **virtual security consultant**. It offers patch management, vulnerability assessment, and network auditing services. It also assists you in asset inventory, change management, risk analysis, and proving compliance.

Features:

- ⌚ Selectively creates custom vulnerability checks
- ⌚ Identifies security vulnerabilities and takes remedial action
- ⌚ Creates different types of scans and vulnerability tests
- ⌚ Helps ensure third party security applications offer optimum protection
- ⌚ Performs network device vulnerability checks



FIGURE 3.50: GFI LanGuard Screenshot

The SAINT vulnerability assessment scanner identifies threats across the network including devices, operating systems, desktop applications, web applications, databases, etc.

Features:

- ☛ Identify vulnerabilities on network devices
- ☛ Detect and fix possible weaknesses in the network security
- ☛ Prevent common system vulnerabilities
- ☛ Demonstrate compliance with current government and industry regulations
- ☛ Perform compliance audits with policies defined by FDCC, USGCB, and DISA

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

<http://www.saintcorporation.com>



Vulnerability Scanning Tool: SAINT

Source: <http://www.saintcorporation.com>

SAINT is an **integrated network tools** for **security administrators**. Using this tool, you can find security vulnerabilities across the network including devices, operating systems, desktop applications, web applications, databases, etc. in a **non-intrusive manner**. It also enables you to gather information such as operating system types and open ports, etc. It allows you to scan and exploit targets with an IPv4, IPv6, and/or URL address.

Features:

- ☛ Detects and fixes possible weaknesses in your network's security
- ☛ Anticipates and prevents common system vulnerabilities
- ☛ Demonstrates compliance with current government and industry regulations such as PCI DSS, NERC, FISMA, SOX, GLBA, HIPAA, and COPPA
- ☛ Performs compliance audits with policies defined by FDCC, USGCB, and DISA

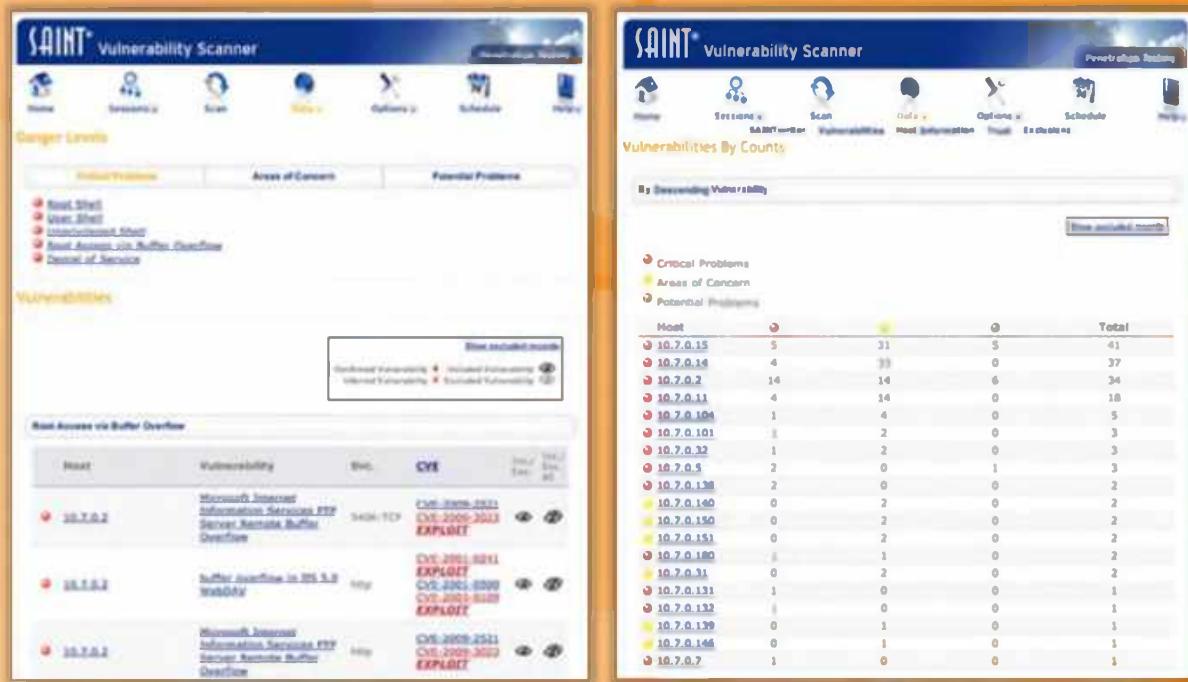


FIGURE 3.51: SAINT Screenshots

Network Vulnerability Scanners

C|EH
Certified Ethical Hacker

 Retina CS http://go.eeye.com	 OpenVAS http://www.openvas.org
 Core Impact Professional http://www.coresecurity.com	 Security Manager Plus http://www.manageengine.com
 MBSA http://www.microsoft.com	 Nexpose http://www.rapid7.com
 Shadow Security Scanner http://www.safety-lab.com	 QualysGuard http://www.qualys.com
 Nsauditor Network Security Auditor http://www.nsauditor.com	 Security Auditor's Research Assistant (SARA) http://www.arc.com

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

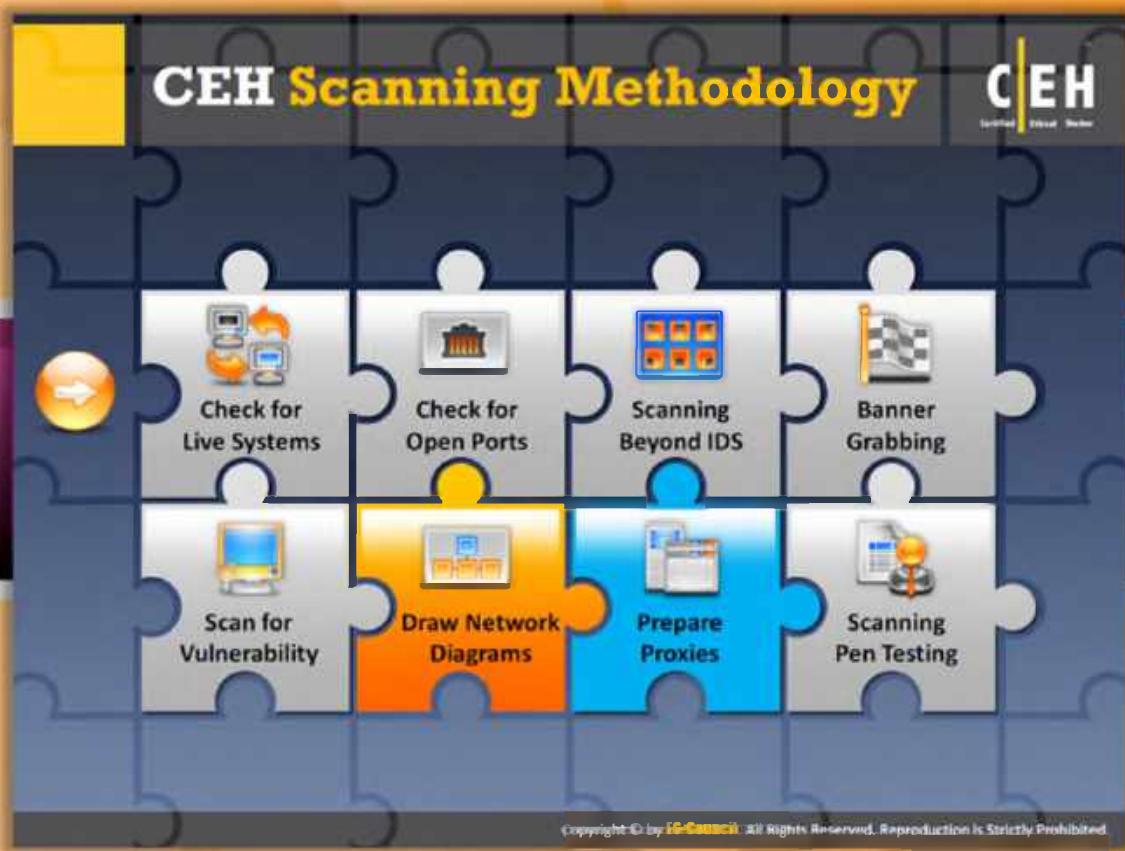


Network Vulnerability Scanners

Network vulnerability scanners are the tools that assist you in identifying the vulnerabilities in the **target network** or **network resources**. These scanners help you in vulnerability assessment and network auditing. Using these scanners, you can find vulnerabilities in networks, wired or wireless, operating systems, security configuration, server tuning, open ports, applications, etc.

A few network vulnerability scanners and their home sites are mentioned as follows, using which you can perform network scanning:

- ⌚ Retina CS available at <http://go.eeye.com>
- ⌚ Core Impact Professional available at <http://www.coresecurity.com>
- ⌚ MBSA available at <http://www.microsoft.com>
- ⌚ Shadow Security Scanner available at <http://www.safety-lab.com>
- ⌚ Nsauditor Network Security Auditor available at <http://www.nsauditor.com>
- ⌚ OpenVAS available at <http://www.openvas.org>
- ⌚ Security Manager Plus available at <http://www.manageengine.com>
- ⌚ Nexpose available at <http://www.rapid7.com>
- ⌚ QualysGuard available at <http://www.qualys.com>
- ⌚ Security Auditor's Research Assistant (SARA) available at <http://www.arc.com>

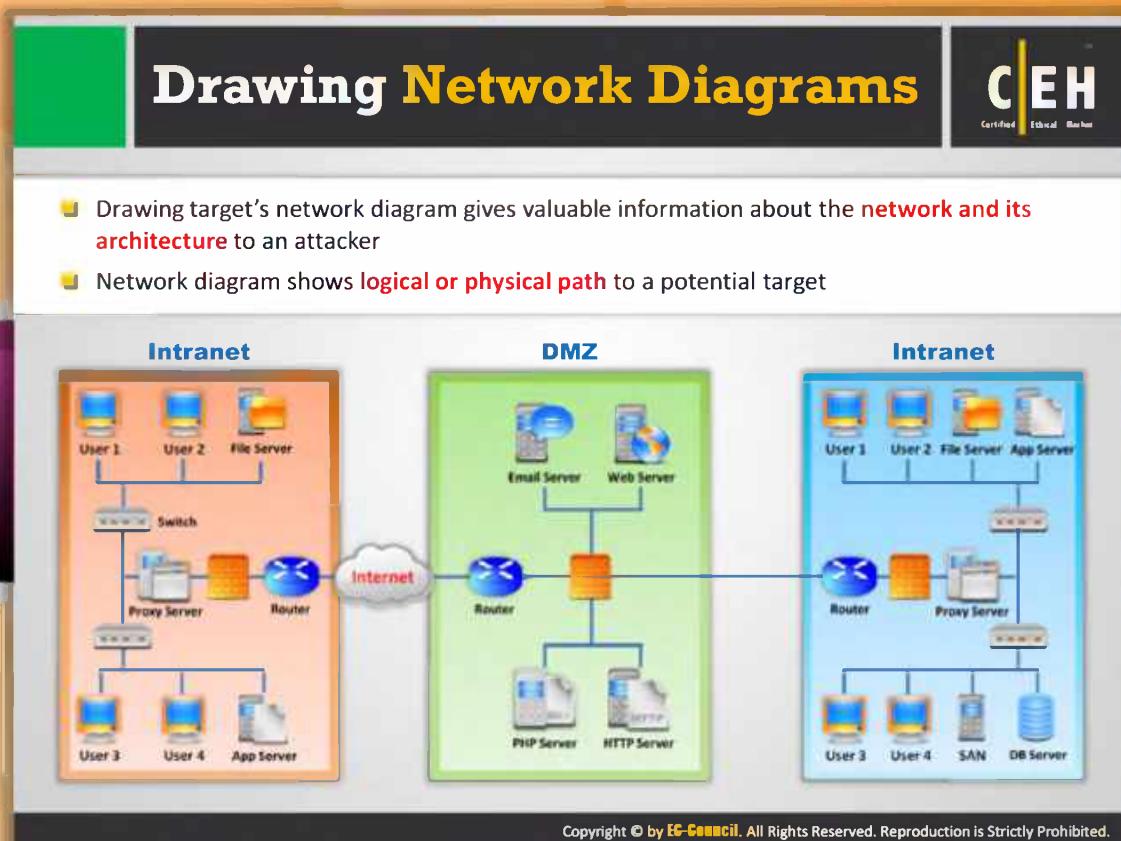


CEH Scanning Methodology

So far, we discussed various scanning concepts such as sources to be scanned, tools that can be used for scanning, and vulnerability scanning. Now we will discuss the network diagram, an important diagram that enables you to analyze the **complete network topology**.

 Check for Live Systems	 Scan for Vulnerability
 Check for Open Ports	 Draw Network Diagrams
 Scanning Beyond IDS	 Prepare Proxies
 Banner Grabbing	 Scanning Pen Testing

This section highlights the importance of the network diagram, how to draw the network diagram or maps, how attackers can use these launching attacks, and the tools that can be used to draw network maps.



Drawing Network Diagrams

The mapping of networks into diagrams helps you to **identify the topology** or the architecture of the target network. The network diagram also helps you to trace out the path to the target host in the network. It also allows you to understand the position of firewalls, routers, and other **access control devices**. Based on the network diagram, the attacker can analyze the target **network's topology** and **security mechanisms**. It helps an attacker to see the firewalls, IDSs, and other security mechanisms of the target network. Once the attacker has this information, he or she can try to figure out the vulnerabilities or weak points of those security mechanisms. Then the attacker can find his or her way into the target network by exploiting those security weaknesses.

The network diagram also helps network administrators manage their networks. Attackers use network discovery or mapping tools to draw network diagrams of target networks.

The following figure depicts an example of a network diagram:

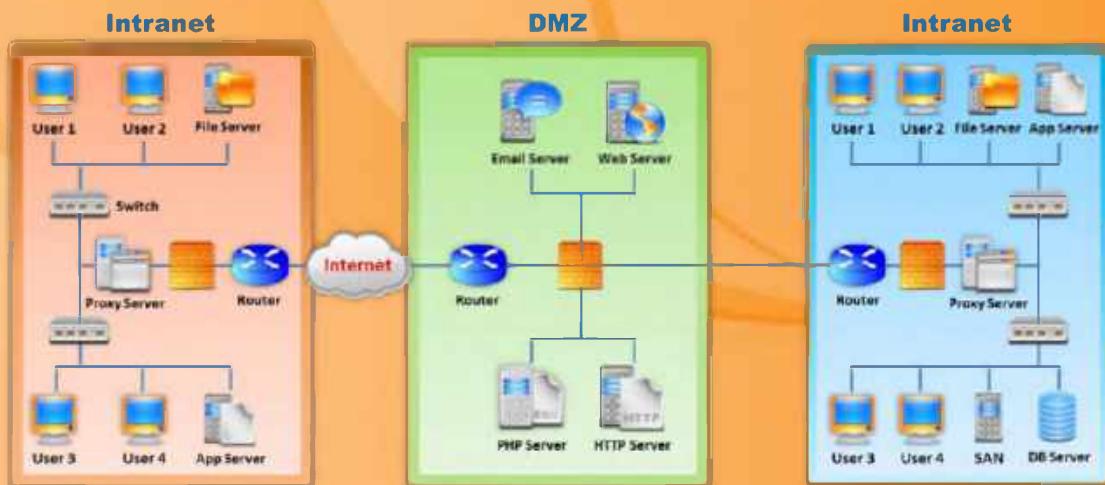


FIGURE 3.52: Network Diagram

The screenshot shows the SolarWinds LANsurveyor software interface. At the top, there's a banner with the text "Network Discovery Tool: LANsurveyor" and the CEH logo. Below the banner, a callout bubble highlights the tool's ability to discover networks and produce comprehensive network diagrams. A list of features is provided, including Auto-generate Network Maps, Export Network Maps to Visio, Auto-detect Changes, Inventory Management, Network Regulatory Compliance, Network Topology Database, and Multi-level Network Discovery. To the right of the callout is a screenshot of the software's main window, which displays a hierarchical network map with various nodes and connections. The bottom of the window shows the URL <http://www.solarwinds.com> and a copyright notice from EC-Council.



Network Discovery Tool: LANsurveyor

Source: <http://www.solarwinds.com>

LANsurveyor allows you to **automatically discover** and **create a network map** of the target network. It is also able to display in-depth connections like **OSI Layer 2** and **Layer 3** topology data such as displaying switch to switch, switch to node, and switch to router connection. You can export the network map created into Microsoft Office Visio. It can also keep track of changes that occur in the network. It allows the user to perform inventory management of hardware and software assets.

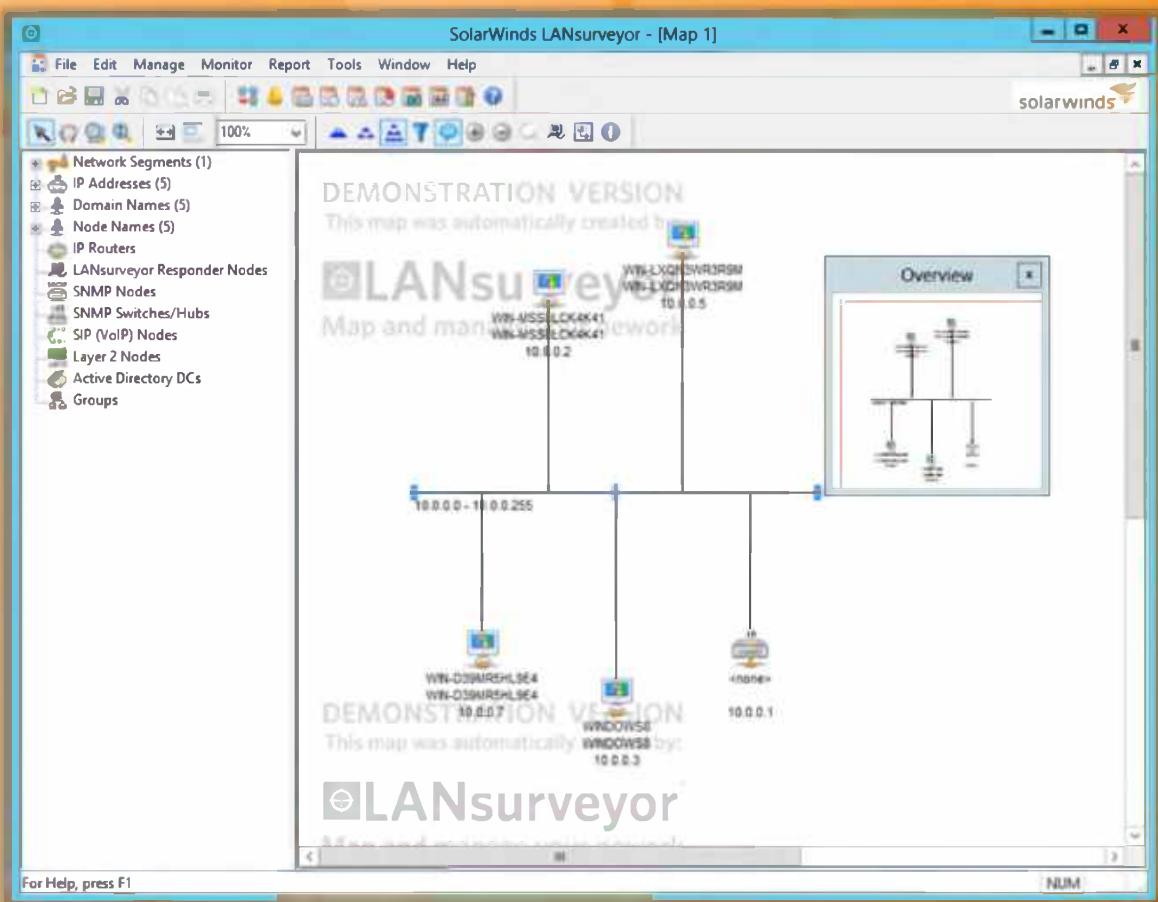


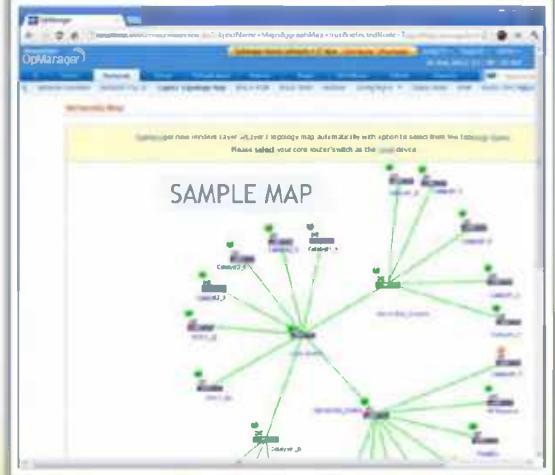
FIGURE 3.53: LANsurveyor Screenshot

Network Discovery Tool: OpManager

OpManager is a network monitoring software that offers advanced **fault and performance management** functionality across critical **IT resources** such as routers, WAN links, switches, firewalls, VoIP call paths, physical servers, virtual servers, domain controllers, and other IT infrastructure devices

Features

- Availability and Uptime Monitoring
- Network Traffic Analysis
- IP Address Management
- Switch Port Mapper
- Network Performance Reporting
- Network Configuration Management
- Exchange Server Monitoring
- Active Directory Monitoring
- Hyper-V Monitoring
- SQL Server Monitoring



http://www.manageengine.com

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



Network Discovery Tool: OpManager

Source: <http://www.manageengine.com>

OpManager is basically a **network performance management** and **monitoring tool** that offers advanced fault and performance management functionality across critical IT resources such as routers, WAN links, switches, firewalls, VoIP call paths, physical servers, virtual servers, domain controllers, and other IT infrastructure devices. This tool is helpful in discovering the specific network automatically. It can also present a live network diagram of your network.

Here are some of the features of OpManager:

- ➊ Availability and uptime monitoring
- ➋ Network traffic analysis
- ➌ IP address management
- ➍ Switch port mapper
- ➎ Network performance reporting
- ➏ Network configuration management
- ➐ Exchange server monitoring

- ⌚ Active directory monitoring
- ⌚ Hyper-V monitoring
- ⌚ SQL Server monitoring

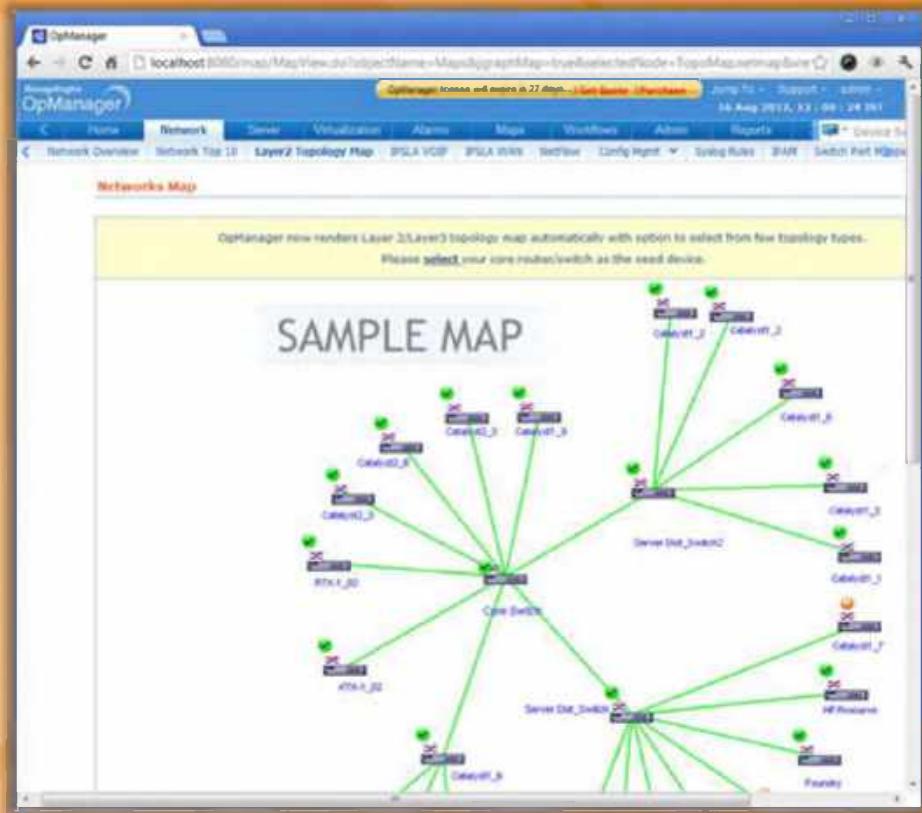
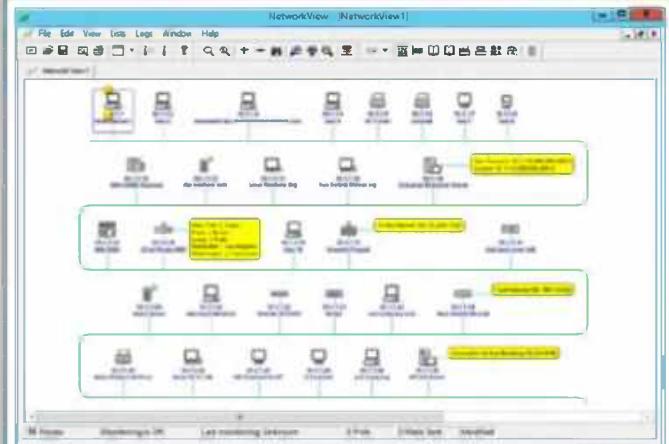


FIGURE 3.54: OpManager showing Sample Map

Network Discovery Tool: NetworkView



NetworkView is a network discovery and management tool for Windows. It allows users to discover TCP/IP nodes and routes using DNS, SNMP, ports, NetBIOS, and WMI. The software provides monitoring, alerting, and reporting features, and includes an SNMP MIB browser, WMI browser, and port scanner.

<http://www.networkview.com>

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



Network Discovery Tool: NetworkView

Source: <http://www.networkview.com>

NetworkView is a **network discovery** and **management tool** for Windows.

Its key features include:

- ☛ Discover TCP/IP nodes and routes using DNS, SNMP, Ports, NetBIOS, and WMI
- ☛ Get **MAC addresses** and NIC manufacturer names
- ☛ Monitor nodes and receive alerts
- ☛ Document with printed **maps** and **reports**
- ☛ Control and secure your network with the **SNMP MIB browser**, the **WMI browser**, and the **port scanner**

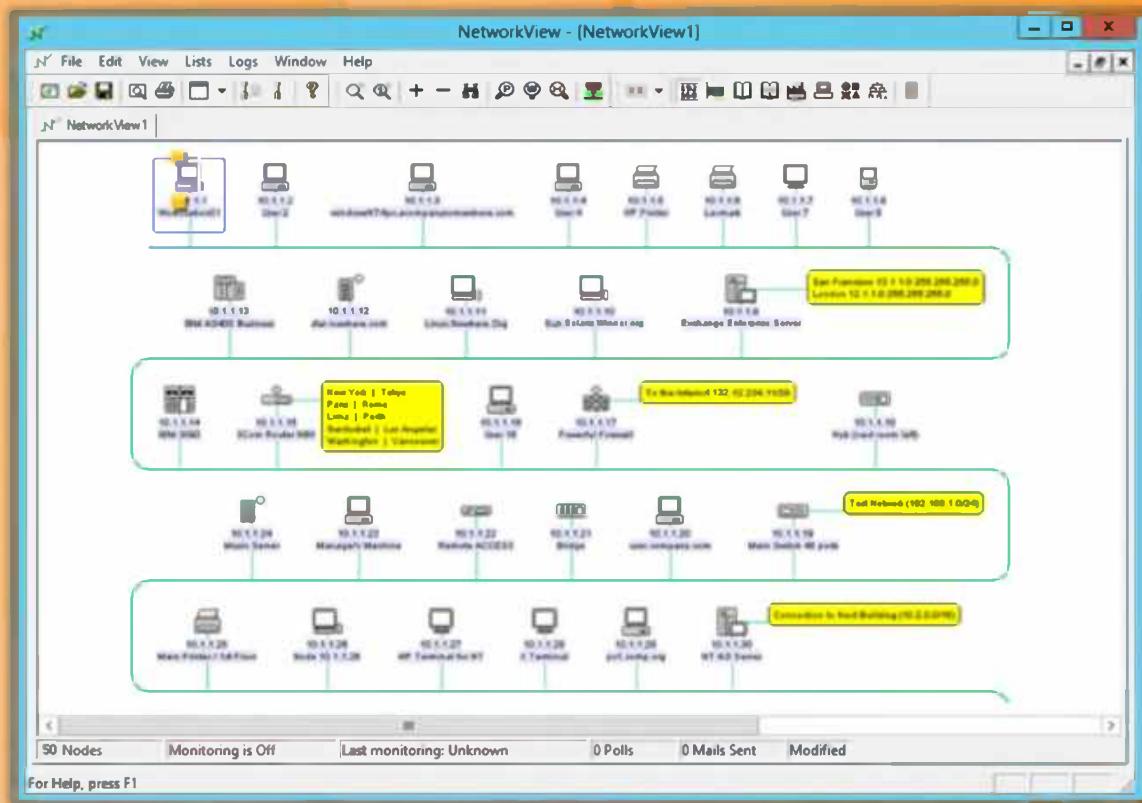
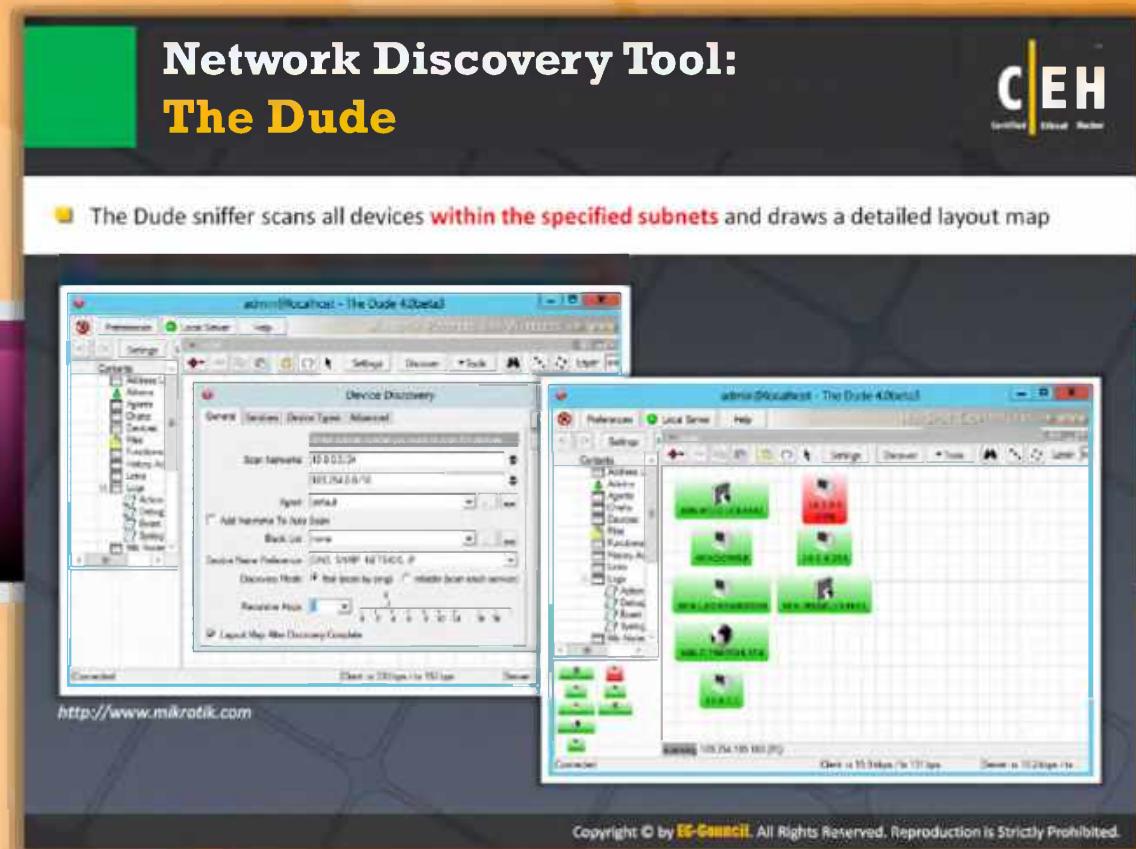


FIGURE 3.55: NetworkView Screenshot



Network Discovery Tool: The Dude

Source: <http://www.mikrotik.com>

The Dude will **automatically scan** all devices within specified subnets, draw and lay out a map of your networks, monitor services of your devices, and alert you in case any service has problems.

A few features of the Dude include:

- Auto network discovery and layout
- Discovers any type or brand of device
- Device, link monitoring, and notifications
- Allows you to draw your own maps and add custom devices
- Supports SNMP, ICMP, DNS, and TCP monitoring for devices that support it
- Direct access to remote control tools for device management
- Supports remote Dude server and local client



FIGURE 3.56: The Dude Screenshots

Network Discovery and Mapping Tools



	LANState http://www.10-strike.com		HP Network Node Manager i Software http://www8.hp.com
	FriendlyPinger http://www.kilievich.com		NetMapper http://www.opnet.com
	Ipsonar http://www.lumeta.com		NetBrain Enterprise Suite http://www.netbraintech.com
	CartoReso http://cartoreso.campus.ecp.fr		Spiceworks-Network Mapper http://www.spiceworks.com
	Switch Center Enterprise http://www.lan-secure.com		NetCrunch http://www.adremsoft.com

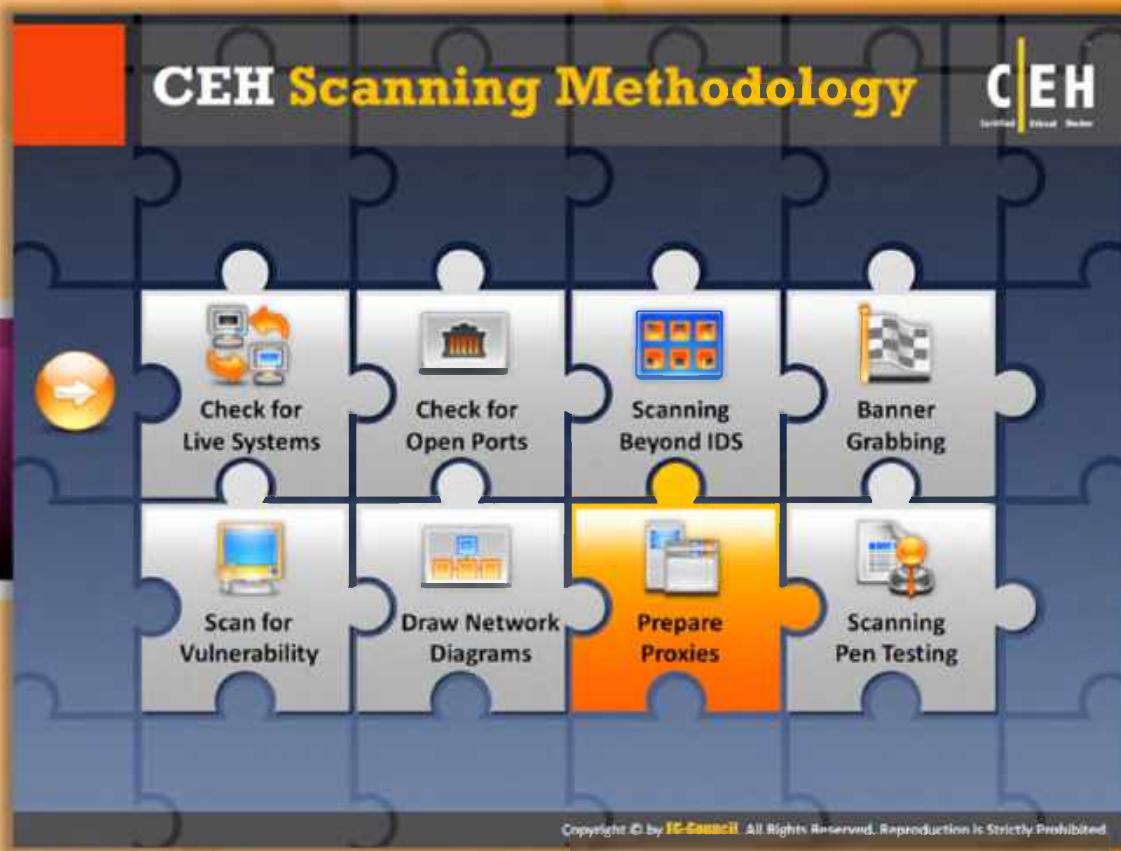
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



Network Discovery and Mapping Tools

Network discovery and mapping tools allow you to view the map of your network. They help you **detect rogue hardware** and **software violations**. It notifies you whenever a particular host becomes active or goes down. Thus, you can also figure out the server outages or problems related to performance. This is the purpose of network discovery and mapping tools in terms of security. The **same tools** can be used by attackers to launch attacks on your network. Using these tools, the attacker draws the network diagram of the target network, analyzes the topology, finds out the vulnerabilities or weak points, and launches an attack by exploiting them. The attacker may use the following tools to create a map of the network:

- ④ LANState available at <http://www.10-strike.com>
- ④ FriendlyPinger available at <http://www.kilievich.com>
- ④ Ipsonar available at <http://www.lumeta.com>
- ④ CartoReso available at <http://cartoreso.campus.ecp.fr>
- ④ Switch Center Enterprise available at <http://www.lan-secure.com>
- ④ HP Network Node Manager i Software available at <http://www8.hp.com>
- ④ NetMapper available at <http://www.opnet.com>
- ④ NetBrain Enterprise Suite available at <http://www.netbraintech.com>
- ④ Spiceworks-Network Mapper available at <http://www.spiceworks.com>
- ④ NetCrunch available at <http://www.adremsoft.com>



CEH Scanning Methodology

So far, we have discussed various means of scanning and the sources to be scanned. Now we will discuss proxies and important mechanisms used by attackers to access the restricted sources and also to avoid their identity.

 Check for Live Systems	 Scan for Vulnerability
 Check for Open Ports	 Draw Network Diagrams
 Scanning Beyond IDS	 Prepare Proxies
 Banner Grabbing	 Scanning Pen Testing

This section describes how to prepare proxies and how an attacker can use them to launch attacks.

Proxy Servers

CEH Certified Ethical Hacker

A proxy is a network computer that can serve as an intermediary for connecting with other computers

As a firewall, a proxy protects the local network from outside access

As an IP address multiplexer, a proxy allows the connection of a number of computers to the Internet while having only one IP address

Specialized proxy servers can filter out unwanted content

Proxy servers can be used (to some extent) to anonymize web surfing

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



Proxy Servers

A proxy is a **network computer** that can serve as an intermediary for connecting with other computers. You can use a proxy server in many ways such as:

- ➊ As a firewall, a proxy protects the local network from the outside access
- ➋ As an IP address multiplexer, a proxy allows a number of computers to connect to the Internet when you have only one IP address
- ➌ To anonymize web surfing (to some extent)
- ➍ To filter out unwanted content, such as ads or “unsuitable” material (using specialized proxy servers)
- ➎ To provide some protection against hacking attacks
- ➏ To save bandwidth

Let's see how a proxy server works.

When you use a proxy to request a particular web page on an actual server, it first sends your **request** to the **proxy server**. The proxy server then **sends** your request to the **actual server** on

behalf of your request, i.e., it mediates between you and the actual server to send and respond to the request as shown in the following figure.



FIGURE 3.57: Attacker using Proxy Server

In this process, the proxy receives the communication between the **client** and the **destination** application. In order to take advantage of a proxy server, **client programs** must be configured so they can send their requests to the proxy server instead of the final destination.

Why Attackers Use Proxy Servers?

CEH
Certified Ethical Hacker

- 1 To hide the **source IP address** so that an attacker can hack without any legal corollary
- 2 To mask the **actual source** of the attack by impersonating a fake source address of the proxy
- 3 To **remotely access intranets** and other **website resources** that are normally off limits
- 4 To **interrupt all the requests** sent by an attacker and transmit them to a third destination, hence victims will only be able to identify the proxy server address
- 5 Attackers chain **multiple proxy servers** to avoid detection

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

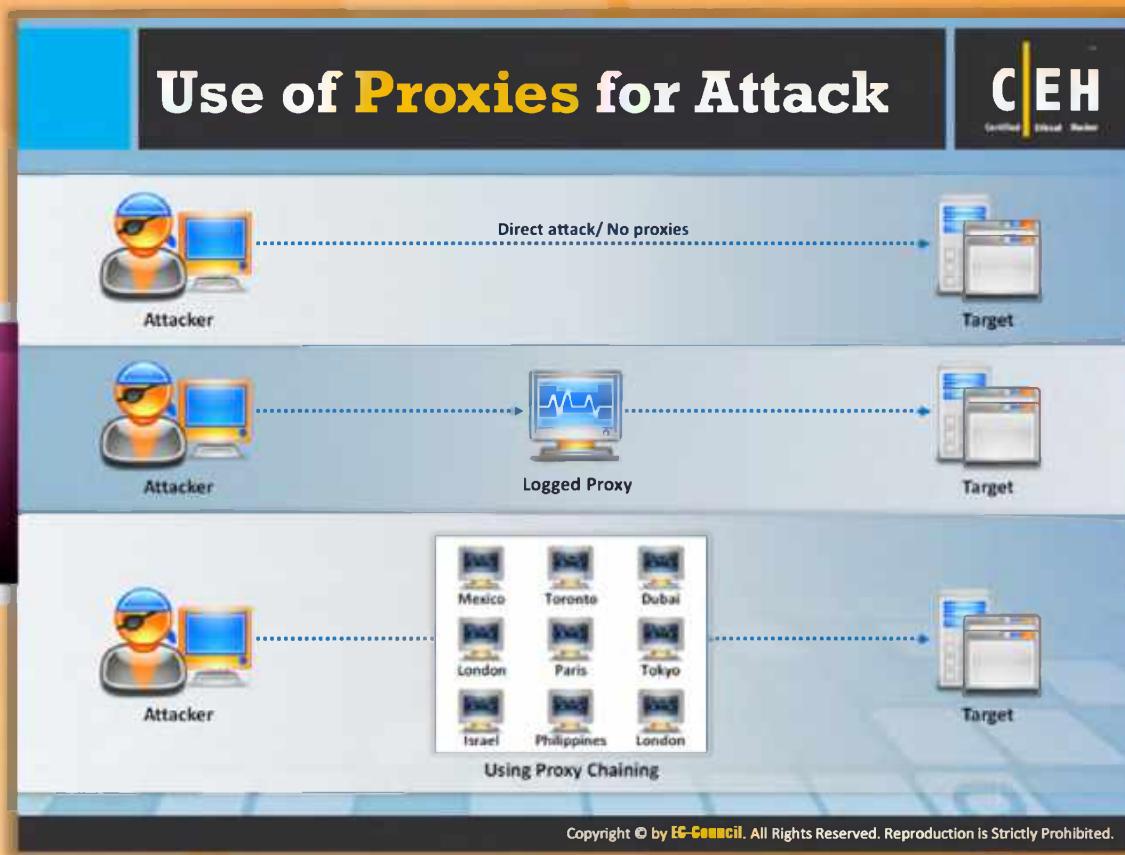


Why Attackers Use Proxy Servers

For an attacker, it is easy to **attack** or **hack** a particular system than to conceal the attack source. So the main challenge for an attacker is to hide his identity so that no one can trace him or her. To conceal the identity, the attacker uses the proxy server. The main cause behind using a proxy is to **avoid detection of attack evidence**. With help of the proxy server, an attacker can **mask** his or her **IP address** so that he or she can hack the computer system without any fear of legal repercussion. When the attacker uses a proxy to connect to the destination, the proxy's source address will be recorded in the server logs instead of the actual source address of the attacker.

In addition to this, the reasons for which attackers use proxy servers include:

- Attacker appears in a victim server's log files with a fake source address of the proxy rather than with the attacker's actual address
- To remotely access intranets and other website resources that are normally off limits
- To interrupt all the requests sent by an attacker and transmit them to a third destination, hence victims will only be able to identify the proxy server address
- To use multiple proxy servers for scanning and attacking, making it difficult for administrators to trace the real source of attack



Use of Proxies for Attack

Quite a number of proxies are intentionally open to easy access. **Anonymous proxies** hide the **real IP address** (and sometimes other information) from websites that the user visits. There are two types of **anonymous proxies**: One that can be used in the same way as the non-anonymous proxies and others that are web-based anonymizers.

Let's see how many different ways that attackers can use proxies to commit attacks on the target.

Case 1: In the first case, the attacker performs attacks directly without using proxy. The attacker may be at risk to be traced out as the server logs may contain information about the IP address of the source.



FIGURE 3.58: Attacker Communicating with Target Directly (No Proxy)

Case 2: The attacker uses the proxy to fetch the target application. In this case, the server log will show the IP address of the proxy instead of the attacker's IP address, thereby hiding his or

her identity; thus, the attacker will be at minimum risk of being caught. This will give the attacker the chance to be anonymous on the Internet.

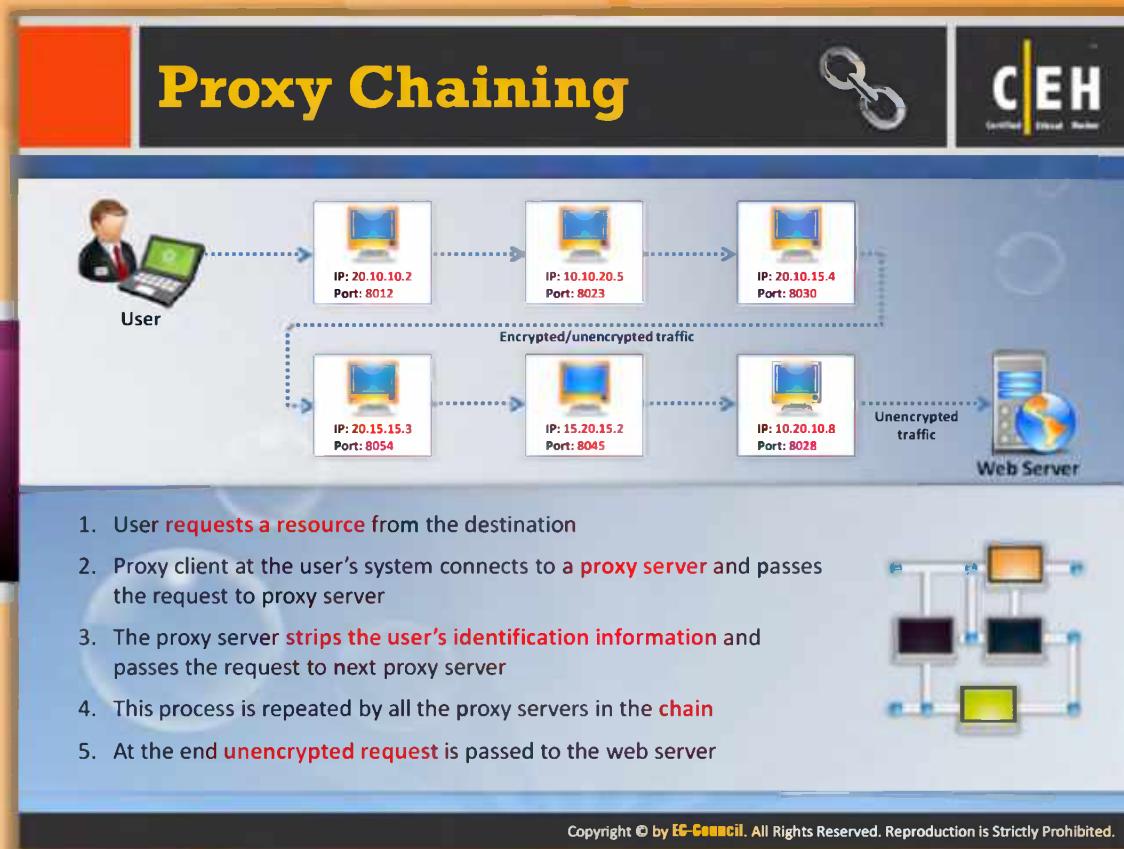


FIGURE 3.59: Attacker Communicating with Target through Proxy

Case 3: To become more anonymous on the Internet, the attacker may use the proxy chaining technique to fetch the target application. If he or she uses proxy chaining, then it is highly difficult to trace out his or her IP address. Proxy chaining is a technique of using more numbers of proxies to fetch the target.



FIGURE 3.60: Attacker using Proxy Chaining for the attack



Proxy Chaining

Proxy chaining helps you to become **more anonymous** on the Internet. Your anonymity on the Internet depends on the number of proxies used for fetching the target application. If you use a larger number of **proxy servers**, then you will become more anonymous on the Internet and vice versa.

When the attacker first requests the proxy server1, this proxy server1 in turn requests another proxy server2. The proxy server1 strips the user's identification information and passes the request to the next proxy server. This may again request another proxy server, server3, and so on, up to target server, where finally the request is sent. Thus, it forms the chain of the proxy server to reach the destination server as shown in the following figure:

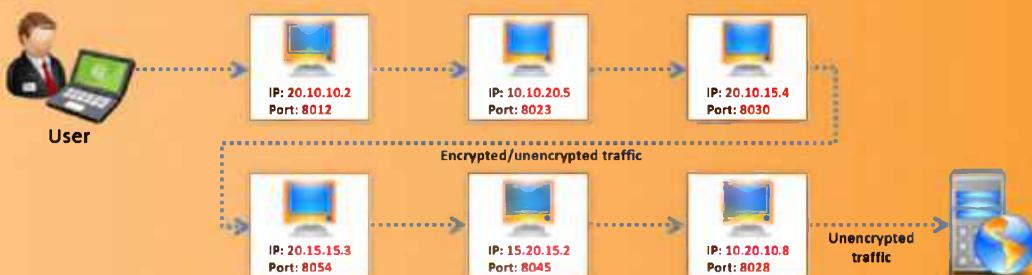
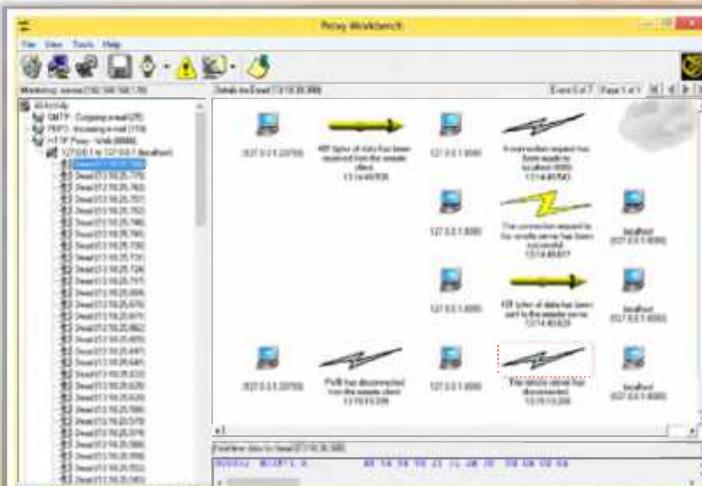


FIGURE 3.61: Proxy Chaining

Proxy Tool: Proxy Workbench

Proxy Workbench is a proxy server that **displays data passing through it in real time**, allows you to drill into particular TCP/IP connections, view their history, save the data to a file, and view the socket connection diagram



The screenshot shows the Proxy Workbench application window. On the left, there's a tree view of monitoring sessions. The main pane displays a socket connection diagram with two hosts: 192.168.1.100 (client) and 192.168.1.101 (server). Arrows indicate data flow between them. Below the diagram, a timeline shows specific events: "401 value of data has been received from the remote client 13:16:40(EST)" and "401 value of data has been sent to the remote server 13:16:40(EST)". A message at the bottom says "Puff has disconnected from the remote client 13:16:40(EST)". The status bar at the bottom shows "Proxy Workbench 1.0.0.1.0.0" and "Windows - Microsoft Internet Explorer".

<http://proxyworkbench.com>

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



Proxy Tool: Proxy Workbench

Source: <http://proxyworkbench.com>

Proxy Workbench is a **proxy server** that **displays the data passing** through it in real time, allows you to drill into particular TCP/IP connections, view their history, save the data to a file, and view the socket connection diagram. The socket connection diagram is an animated graphical history of all of the events that took place on the socket connection. It is able to handle **HTTPS (secure sockets)** and **POP3** natively.

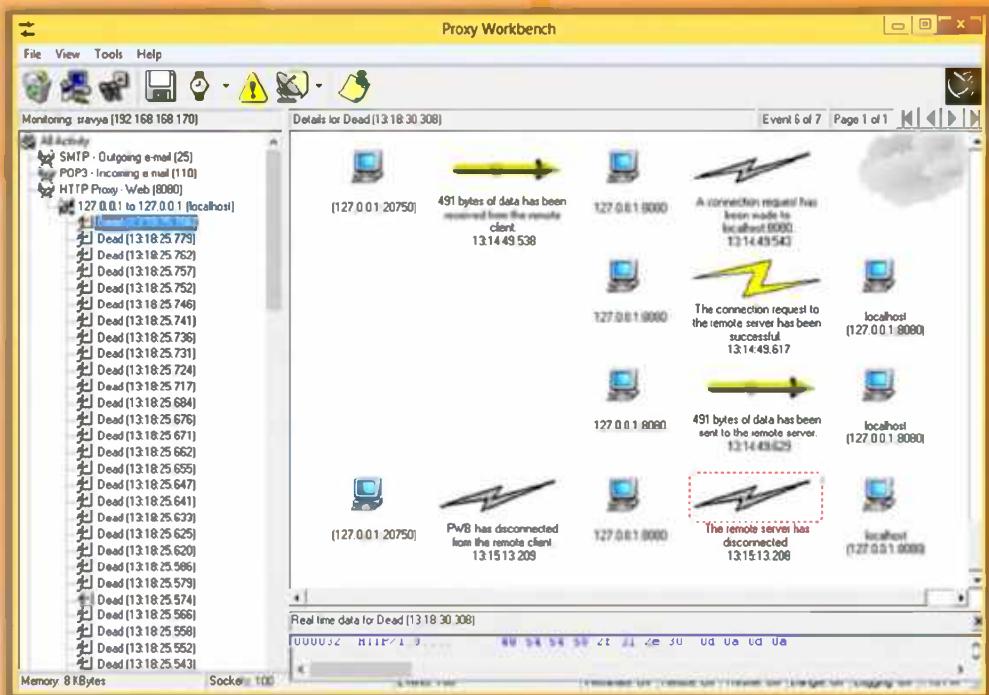


FIGURE 3.62: Proxy Workbench Screenshot



Proxy Tool: Proxifier

Source: <http://www.proxifier.com>

Proxifier allows **network applications** that do not support working through proxy servers to operate through a **SOCKS** or **HTTPS** proxy and chains. It allows you to surf websites that are restricted or blocked by your government, organization, etc. by bypassing the firewalls rules.

Features:

- ❑ You can access the Internet from a restricted network through a proxy server gateway
- ❑ It hides your IP address
- ❑ It can work through a chain of proxy servers using different protocols
- ❑ It allows you to bypass firewalls and any access control mechanisms

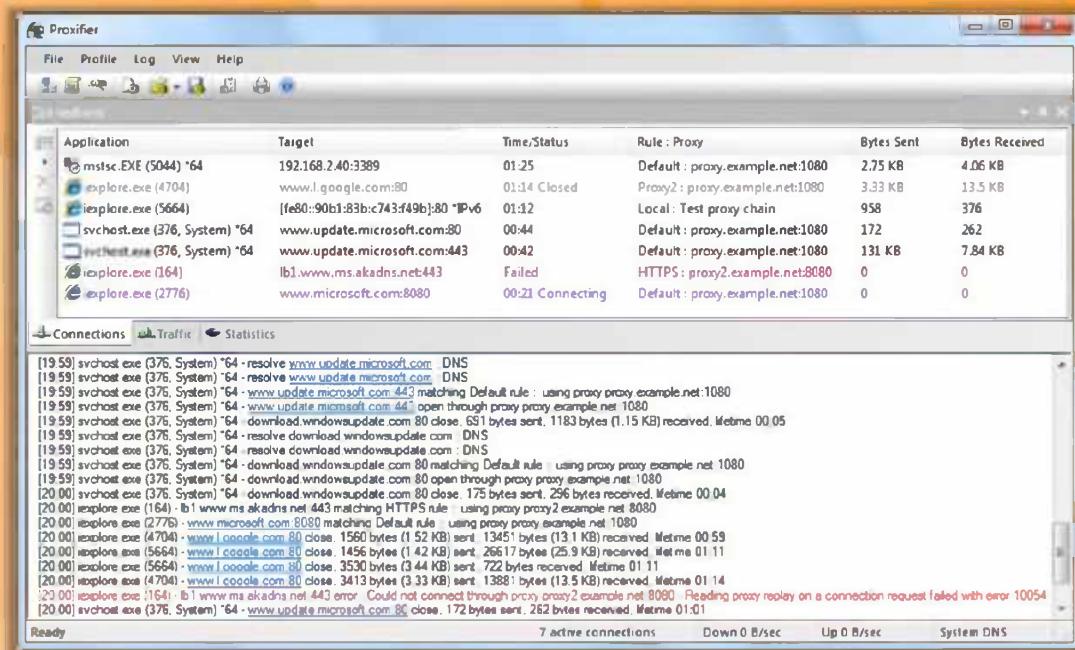
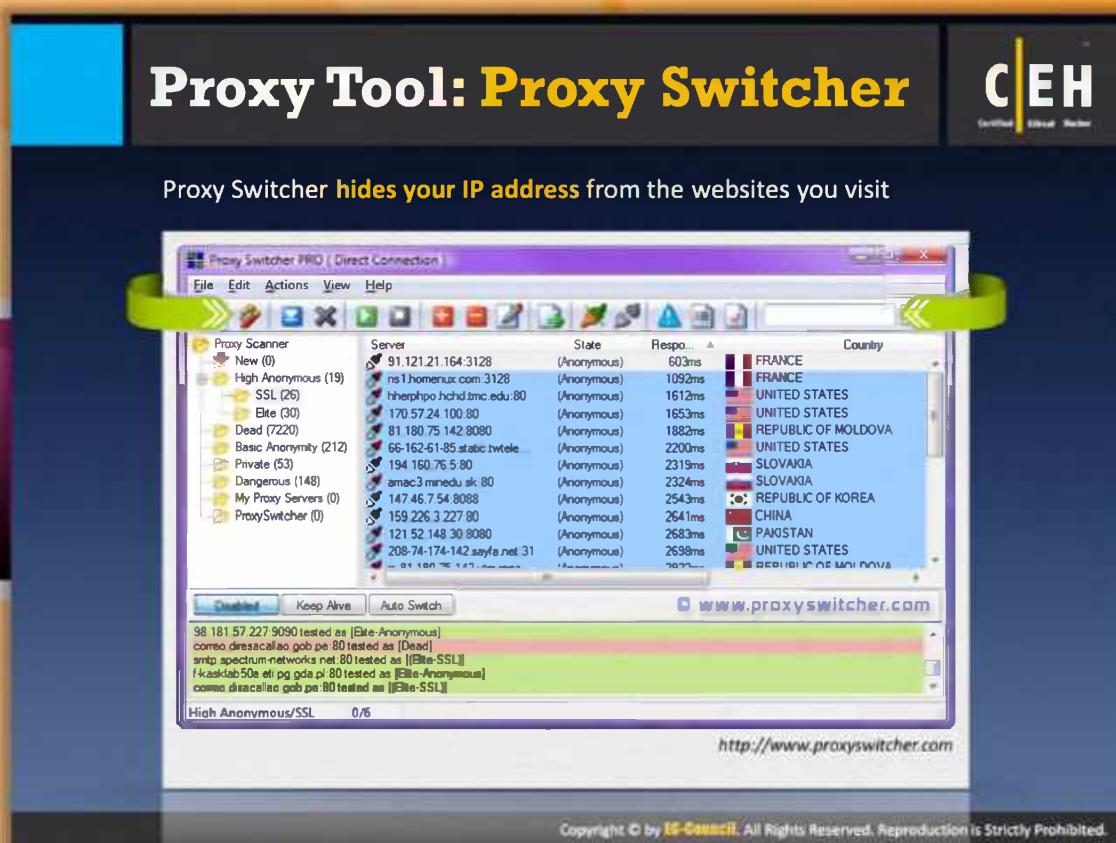


FIGURE 3.63: Proxifier Screenshot



Proxy Tool: Proxy Switcher

Source: <http://www.proxyswitcher.com>

Proxy Switcher allows you to **surf anonymously** on the Internet without disclosing your IP address. It also helps you to access various sites that have been **blocked in the organization**. It avoids all sorts of limitations imposed by sites.

Features:

- ❑ It hides your IP address
- ❑ It allows you to access restricted sites
- ❑ It has full support of password-protected servers

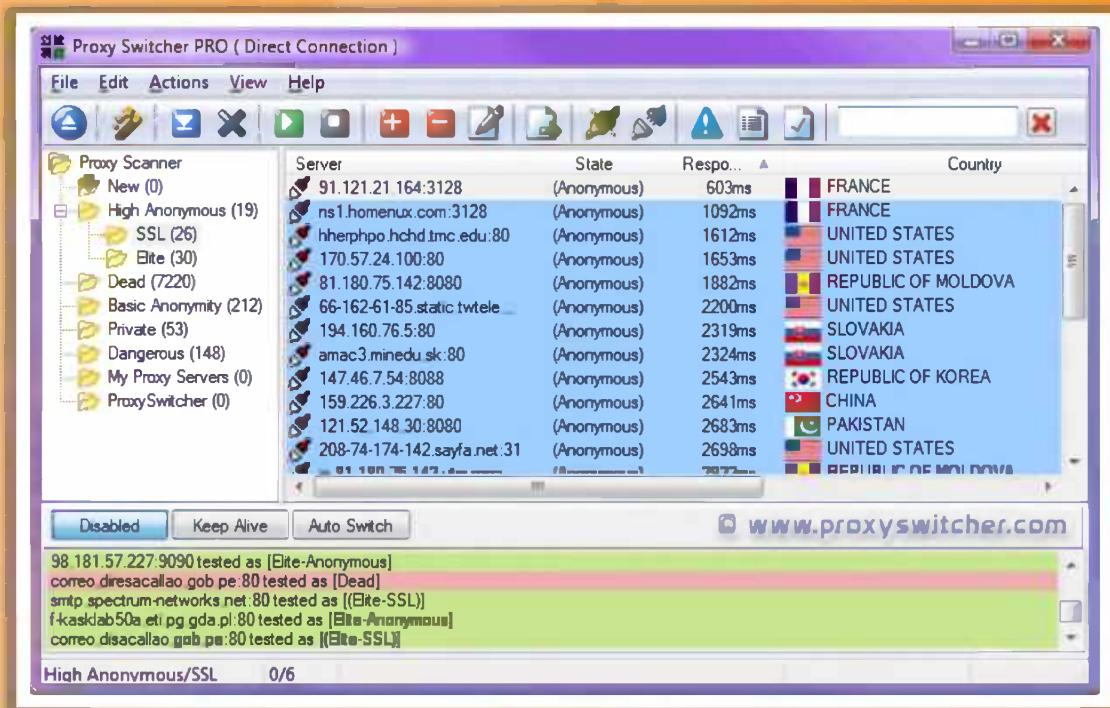
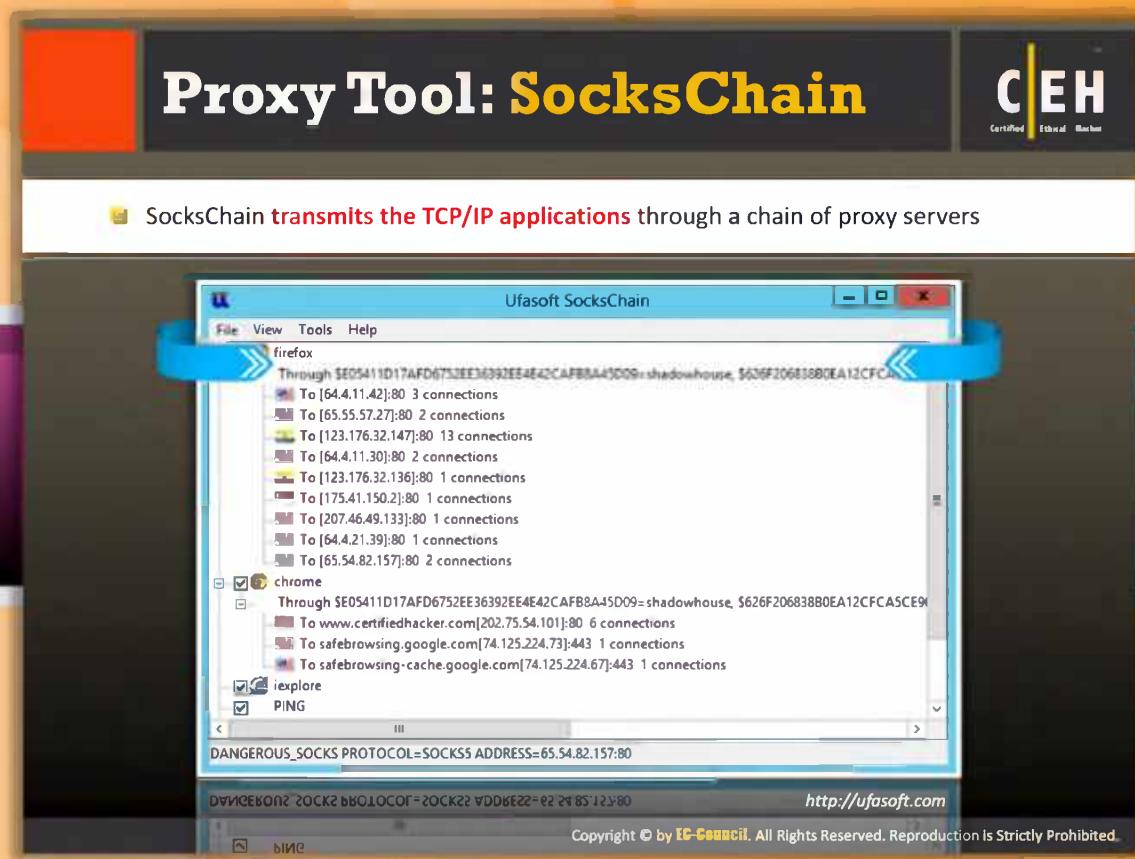


FIGURE 3.64: Proxy Switcher PRO Screenshot



Proxy Tool: SocksChain

Source: <http://ufasoft.com>

SocksChain is a program that allows you to work with any **Internet service** through a chain of **SOCKS** or **HTTP proxies** to hide the real IP address. It can function as a usual SOCKS-server that transmits queries through a chain of proxies. It can be used with client programs that do not support the SOCKS protocol, but work with one **TCP-connection**, such as TELNET, HTTP, IRC, etc. It hides your IP from being displayed in the server's log or mail headers.

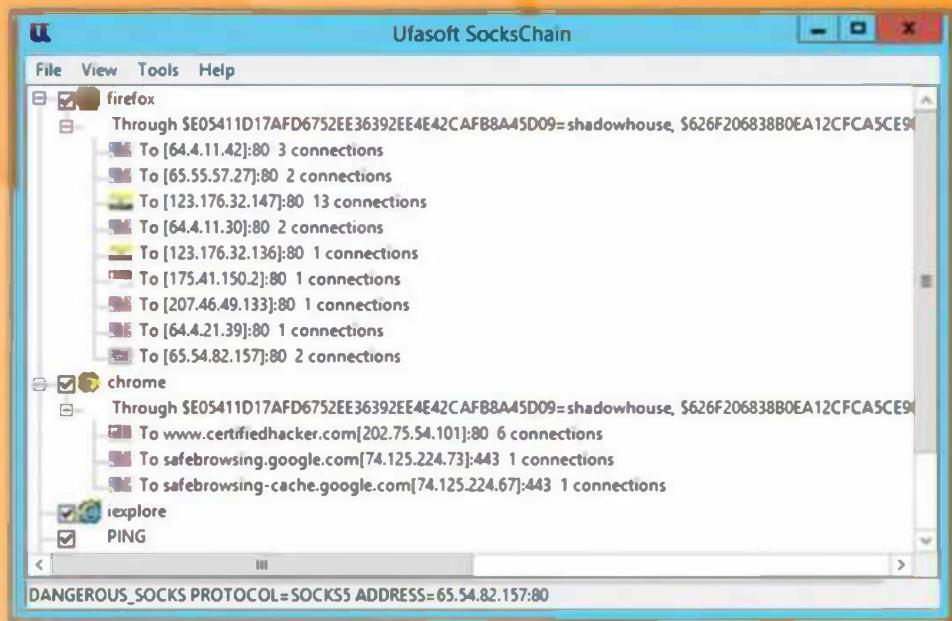
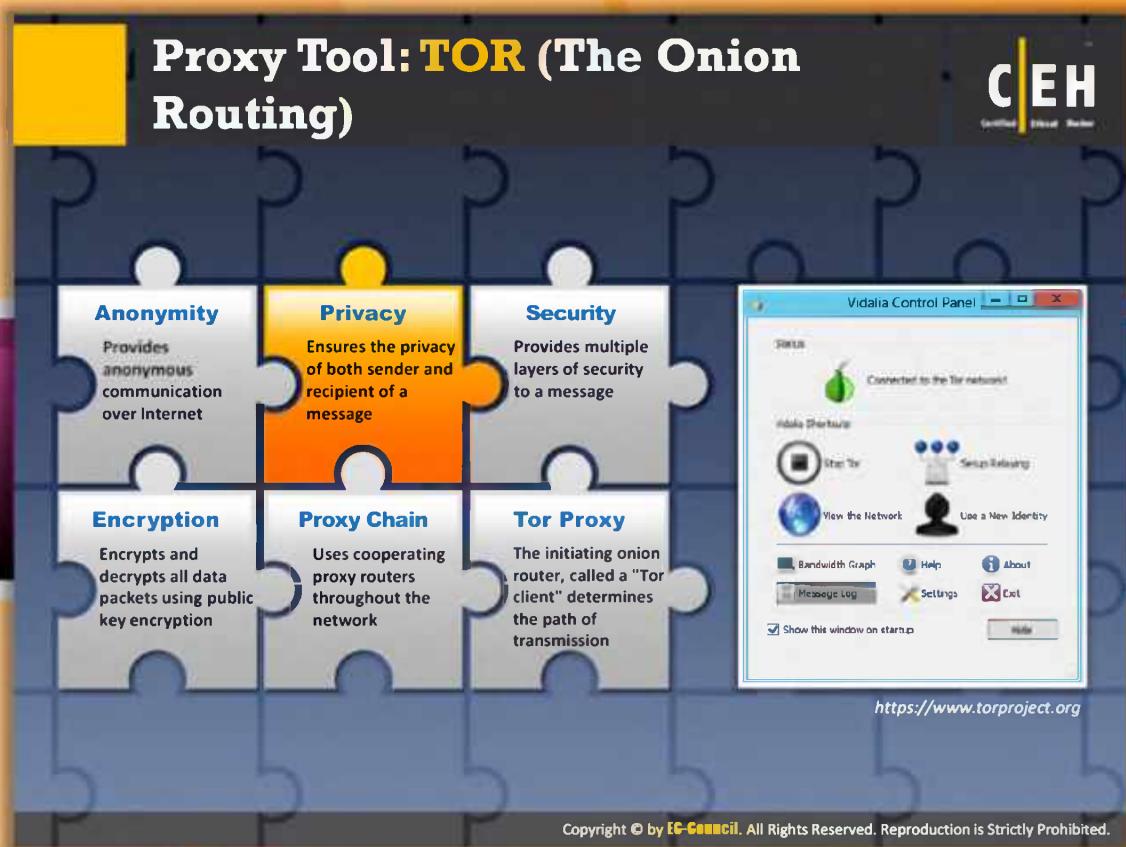


FIGURE 3.65: Ufasoft SocksChain Screenshot



Proxy Tool: TOR (The Onion Routing)

Source: <https://www.torproject.org>

Tor is software and an open network that helps you defend against a form of network surveillance that threatens **personal freedom** and **privacy**, confidential business activities and relationships, and state security known as traffic analysis. You can use Tor to prevent websites from tracking you on the Internet. You can also connect to news sites and instant messaging services when these sites are blocked by your network administrator. Tor makes it difficult to trace your Internet activity as it conceals a user's location or usage.

Features:

- ❑ Provides anonymous communication over the Internet
- ❑ Ensures the privacy of both sender and recipient of a message
- ❑ Provides multiple layers of security to a message
- ❑ Encrypts and decrypts all data packets using public key encryption
- ❑ Uses cooperating proxy routers throughout the network
- ❑ The initiating onion router, called a "Tor client" determines the path of transmission



FIGURE 3.66: Vidalia Control Panel showing the Status

Proxy Tools



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

 Burp Suite http://www.portswigger.net	 Proxy http://www.analogx.com
 Proxy Commander http://www.dlao.com	 Protoport Proxy Chain http://www.protoport.com
 Proxy Tool Windows App http://webproxylist.com	 Proxy+ http://www.proxyplus.cz
 Gproxy http://gpass1.com	 FastProxySwitch http://affinity-tools.com
 Fiddler http://www.fiddler2.com	 ProxyFinder http://www.proxy-tool.com



Proxy Tools

In addition to these proxy tools, there are many more proxy tools intended to allow users to surf the Internet anonymously. A few are listed as follows:

- ⌚ Burp Suite available at <http://www.portswigger.net>
- ⌚ Proxy Commander available at <http://www.dlao.com>
- ⌚ Proxy Tool Windows App available at <http://webproxylist.com>
- ⌚ Gproxy available at <http://gpass1.com>
- ⌚ Fiddler available at <http://www.fiddler2.com>
- ⌚ Proxy available at <http://www.analogx.com>
- ⌚ Protoport Proxy Chain available at <http://www.protoport.com>
- ⌚ Proxy+ available at <http://www.proxyplus.cz>
- ⌚ FastProxySwitch available at <http://affinity-tools.com>
- ⌚ ProxyFinder available at <http://www.proxy-tool.com>

Proxy Tools (Cont'd)



 ProxyFinder Enterprise http://www.proxy-tool.com	 Socks Proxy Scanner http://www.mylanviewer.com
 ezProxy http://www.oclc.org	 Charles http://www.charlesproxy.com
 JAP Anonymity and Privacy http://anon.inf.tu-dresden.de/index_en.html	 UltraSurf http://www.ultrasurf.us
 CC Proxy Server http://www.youngzsoft.net	 WideCap http://widecap.ru
 FoxyProxy Standard https://addons.mozilla.org	 ProxyCap http://www.proxycap.com

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



Proxy Tools (Cont'd)

The list of proxy tools mentioned in the previous slide continues as follows:

- ⌚ ProxyFinder Enterprise available at <http://www.proxy-tool.com>
- ⌚ ezProxy available at <http://www.oclc.org>
- ⌚ JAP Anonymity and Privacy available at http://anon.inf.tu-dresden.de/index_en.html
- ⌚ CC Proxy Server available at <http://www.youngzsoft.net>
- ⌚ FoxyProxy Standard available at <https://addons.mozilla.org>
- ⌚ Socks Proxy Scanner available at <http://www.mylanviewer.com>
- ⌚ Charles available at <http://www.charlesproxy.com>
- ⌚ UltraSurf available at <http://www.ultrasurf.us>
- ⌚ WideCap available at <http://widecap.ru>
- ⌚ ProxyCap available at <http://www.proxycap.com>



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

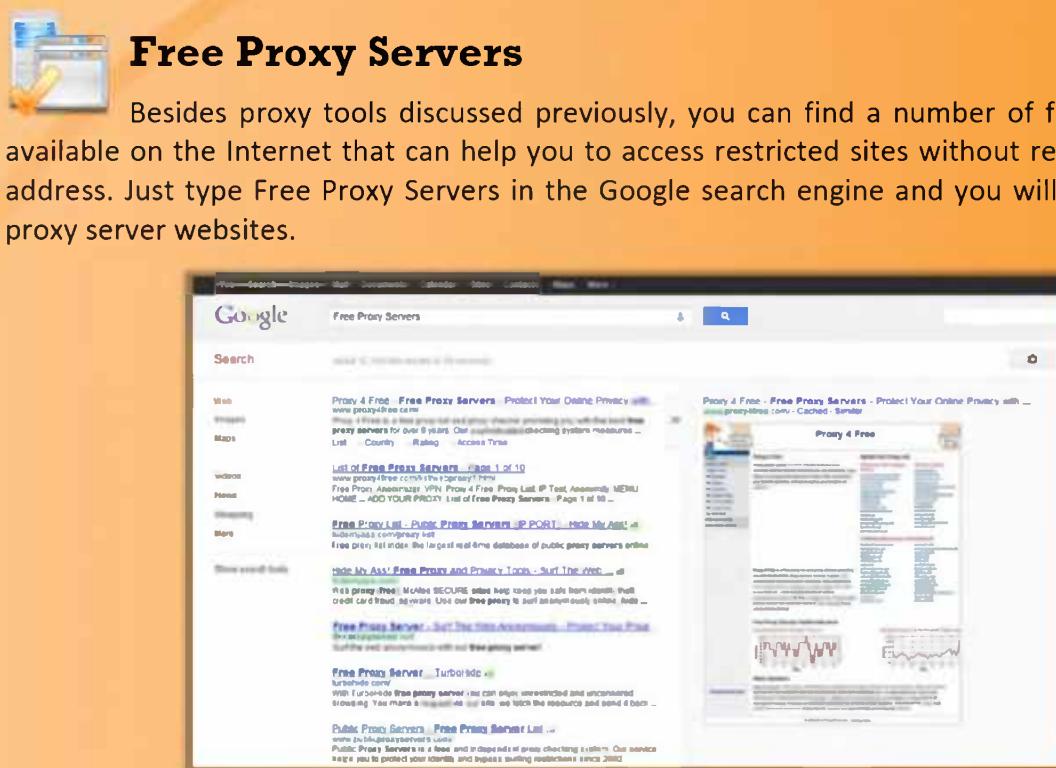


FIGURE 3.67: Google Search showing Free Proxy Servers

HTTP Tunneling Techniques

CEH Certified Ethical Hacker

- HTTP Tunneling technology allows users to **perform various internet tasks** despite the restrictions imposed by firewalls
- Encapsulates data inside **HTTP traffic** (port 80)

End Users use HTTP-Tunnel to transmit or receive data through Firewall

Previously inaccessible servers and services

Racks of HTTP Tunnel Servers

HTTP Tunnel Servers receive and relay the data

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



HTTP Tunneling Techniques

HTTP Tunneling is another technique that allows you to use the Internet despite restrictions imposed by the firewalls. The **HTTP protocol** acts as wrapper for communication channels.

An attacker uses **HTTP tunnel software** to perform HTTP tunneling. It is a client-server-based application used to communicate through the HTTP protocol. This software creates an HTTP tunnel between two machines, using a web proxy option. The technique involves sending POST requests to an "**HTTP server**" and receiving replies.

The attacker uses the client application of HTTP tunnel software installed on his or her system to communicate with other machines. All requests sent through the HTTP tunnel client application go through the HTTP protocol.

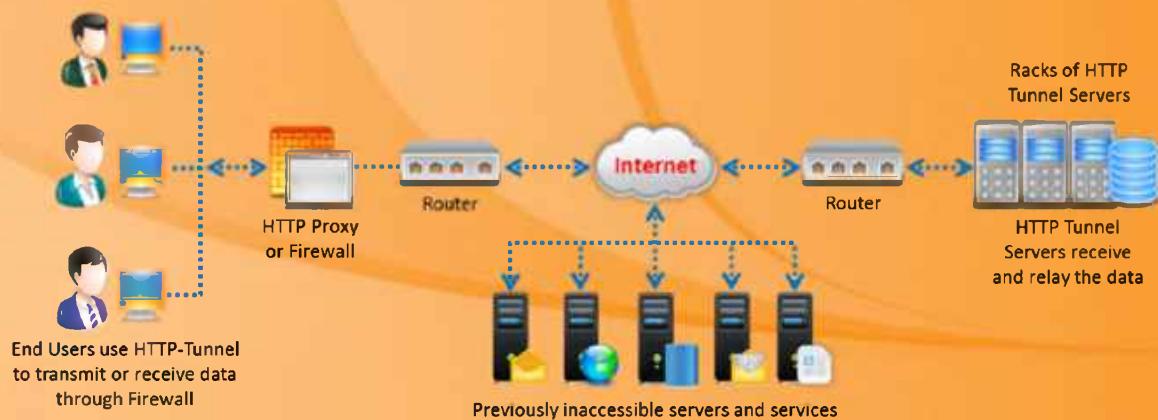
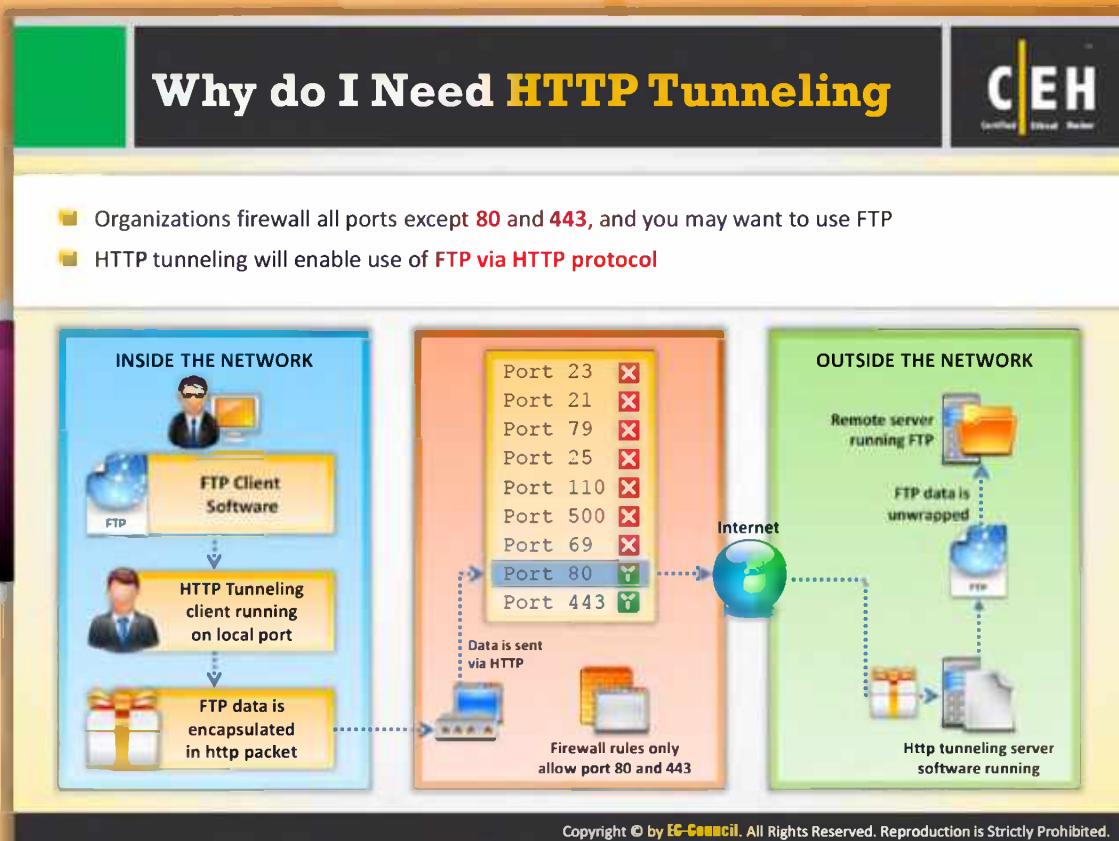


FIGURE 3.68: HTTP Tunneling Process

The HTTP tunneling technique is used in network activities such as:

- ⌚ Streaming video and audio
- ⌚ Remote procedure calls for network management
- ⌚ For intrusion detection alerts
- ⌚ Firewalls



Why do I Need HTTP Tunneling?

HTTP tunneling allows you to use the Internet despite having **firewall restrictions** such as **blocking specific firewall ports** to restrict specific protocol communication. HTTP tunneling helps you to overcome this firewall restriction by sending specific protocol communication through HTTP protocol.

The attacker may use this technique for the following reasons:

- ➊ It assures the attacker that no one will monitor him or her while browsing
- ➋ It helps the attacker to bypass firewall restrictions
- ➌ It ensures secure browsing
- ➍ The attacker can hide his or her IP address from being trapped
- ➎ It assures that it is highly impossible for others to identify him or her online

Suppose the organization has blocked all ports in your firewall and only allows port **80/443**, and you want to use FTP to connect to some remote server on the Internet. In this case, you can send your packets via HTTP protocol as shown in the following figure:

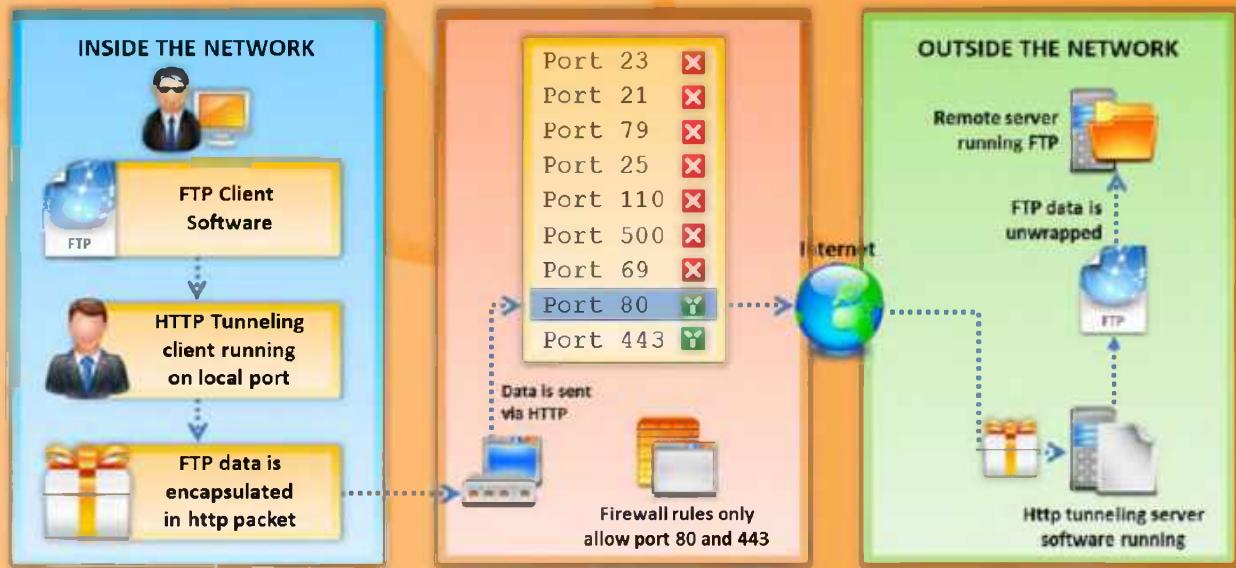
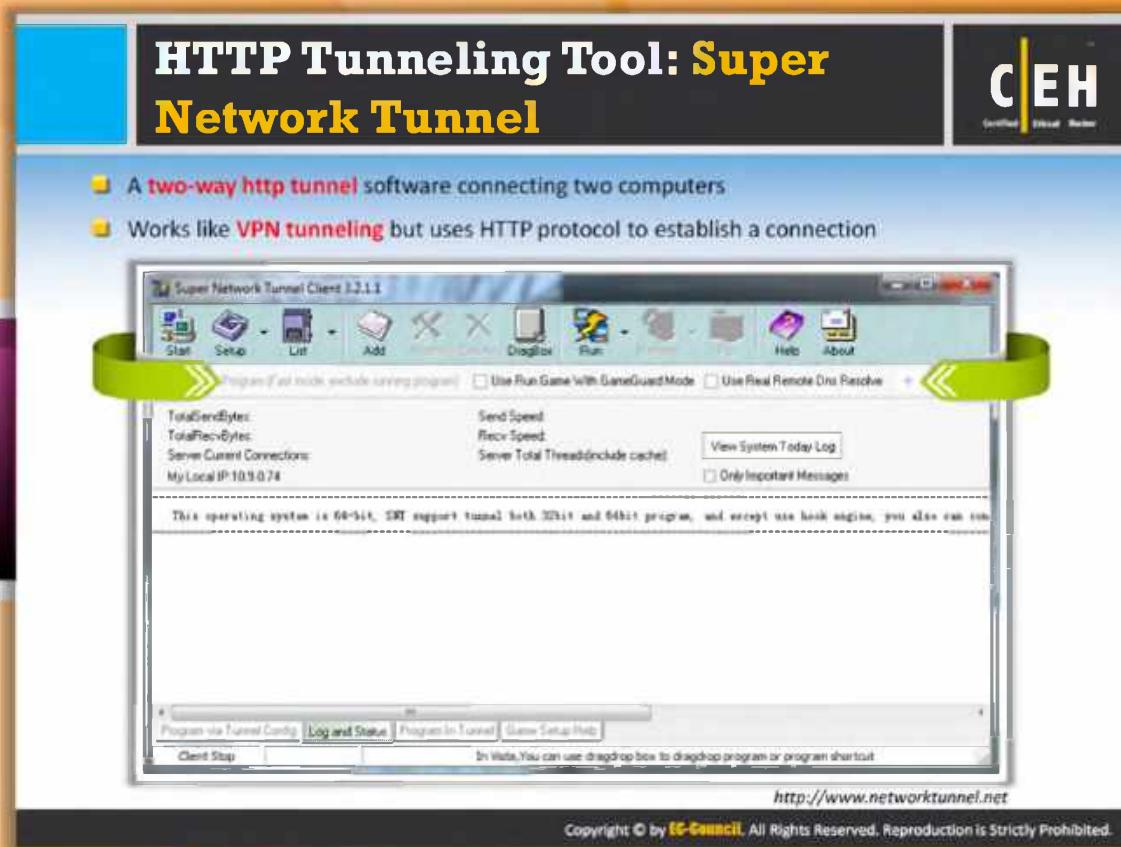


FIGURE 3.69: Effect of HTTP Tunneling on both Inside and Outside the Network



HTTP Tunneling Tool: Super Network Tunnel

Source: <http://www.networktunnel.net>

Super Network Tunnel is a professional HTTP tunneling software, which includes **HTTP tunnel client** and **server software**. It is like secure VPN software that allows you to access your Internet programs without being monitored by your work, school, or the government, and gives you an extra layer of protection against hackers, spyware, or ID theft. It can bypass any firewall.

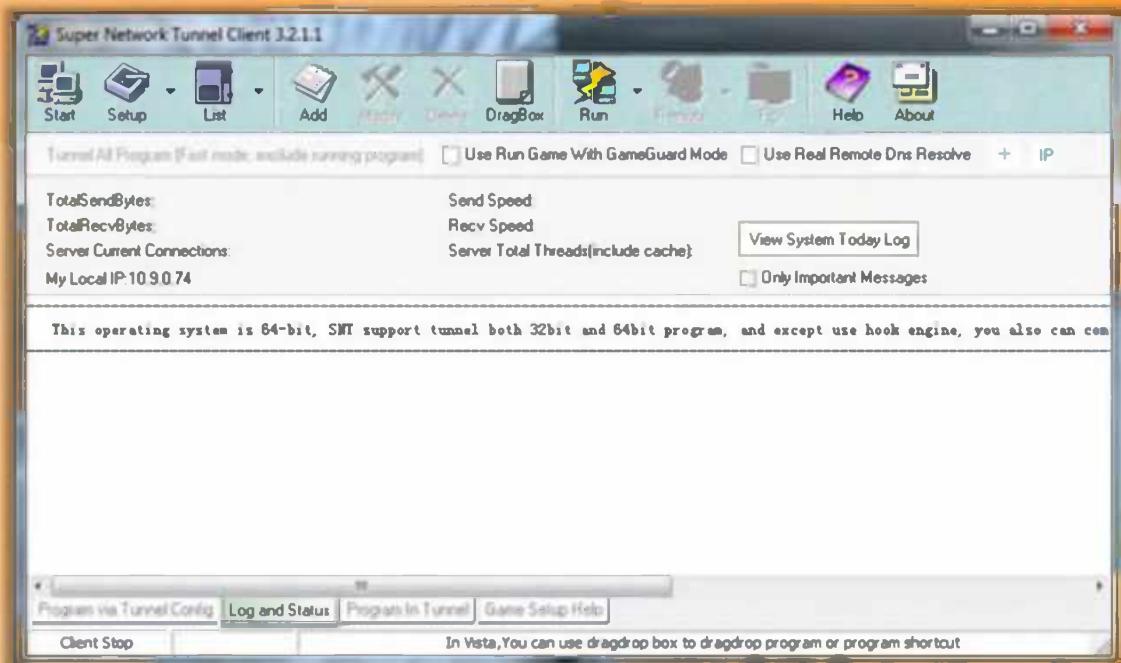


FIGURE 3.70: Super Network Tunnel Screenshot

HTTP Tunneling Tool: HTTP-Tunnel

HTTP-Tunnel acts as a socks server, allowing you to use your Internet applications safely despite restrictive firewalls

SOCKet Secure (SOCKS) is an Internet protocol that routes network packets between a client and server through a proxy server




HTTP-Tunnel Client v4.4.4000

Connections: 123 | Speed Test | Diagnostics | About

123.98.119.189 (Proxy) is now logged in
123.98.119.189 (Remote IP) (via Windows Firewall)

Dear Guests
Click Here
Get Involved
http-tunnel
\$0.99/mo
Get Involved
Free Server Model
FAQ
Upgrades

Proxy Server
 Auto detect
 No Proxy, use a Firewall
 Specific Proxy
 Server Name: IP: Port:
 IP: Port, host or address alias:
 Username:
 Password:
 Maximize (Alt+Shift+F10)
 Access Restrictions
 Turn this ON to use a 256bit SSL connection with this client. This allows you to connect to sites that require SSL/TLS and other security features.
 Wake up to maximize window to HTTP-Tunnel
 Advanced Options
 Set advanced user options, please search Google for info.
 This option will actually improve performance if it is appropriate to your needs. This is used ONLY if you have a server. The connection will be set to the option.
 Proprietary "TCP-NET" command
 Local Port
 TCP-Tunnel listen on Port 1080 for connections from applications. Change this if you need TCP directly to use when you host HTTP (Web). You will also be able to connect your applications directly to TCP-Tunnel.
 1080

<http://www.http-tunnel.com>



HTTP Tunneling Tool: HTTP-Tunnel

Source: <http://www.http-tunnel.com>

HTTP Tunnel acts as a **SOCKS server**, allowing you to access the Internet by **bypassing firewall** restrictions. It is very secure software. Using this software does not allow others to monitor your Internet activities. It hides your IP address; therefore, it does not allow tracing of your system. It allows you the unlimited transfer of data. It runs in your system tray acting as a SOCKS server, managing all data transmissions between the computer and the network.

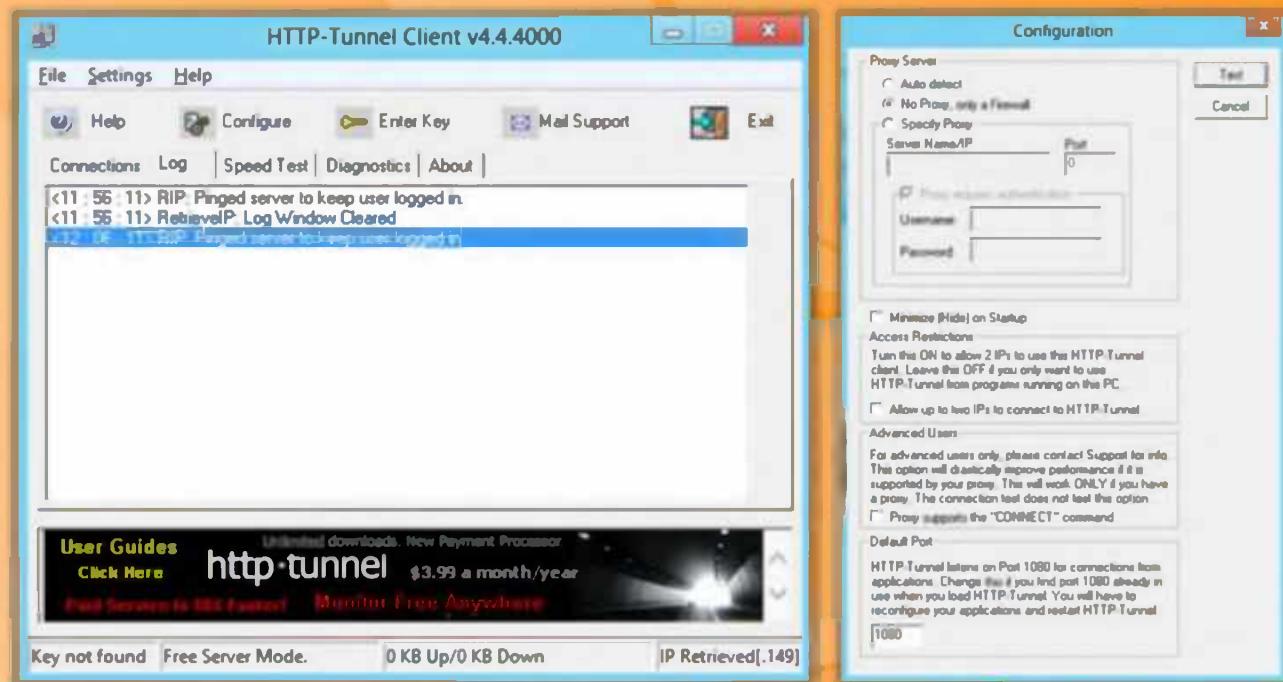


FIGURE 3.71: HTTP-Tunnel Client and Configuration Windows

SSH Tunneling

OpenSSH

Attackers use OpenSSH to **encrypt and tunnel** all the traffic from a local machine to a remote machine to avoid detection by perimeter security controls

Example

```
ssh -f user@certifiedhacker.com -L 5000:certifiedhacker.com:25 -N
```

-f => background mode, user@certifiedhacker.com => user name and server you are logging into, -L 5000:certifiedhacker.com:25 => local-port:host:remote-port, and -N => Do not execute the command on the remote system

- This forwards the local port 5000 to port 25 on certifiedhacker.com encrypted
- Simply point your email client to use localhost:5000 as the SMTP server

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



SSH Tunneling

SSH tunneling is another technique that an attacker can use to **bypass firewall restrictions**. It also helps you hide your IP address on the Internet; therefore, no one can trace or monitor you.

The prerequisite of SSH tunneling is raised from the problems caused by the **public IP address**, the means for accessing computers from anywhere in the world. The computers networked with the public IP address are universally accessible, so they could be attacked by anyone on the global Internet easily and can be **victimized by attackers**. The development of SSH tunneling solves the problems faced by the public IP address.

An SSH tunnel is a link that proceeds traffic from an indiscriminate port on one machine to a remote machine through an intermediate machine. An SSH tunnel comprises an encrypted tunnel, so all your data is encrypted as it uses a secure shell to create the tunnel.

Creating a tunnel for a privately addressed machine needs to implement three basic steps and also requires three machines. The three requisite machines are:

- Local machine
- An intermediate machine with a public IP address
- Target machine with a private address to which the connection must be established

You can create a tunnel as follows:

- ② Start an SSH connection from local machine to the intermediate machine with public IP address.
- ③ Instruct the SSH connection to wait and observe traffic on the local port, and use intermediate machine to send the traffic to an explicit port on the target machine with a private address. This is called port acceleration or port forwarding.
- ④ On the local machine, select the application that you want to use for connection with the remote machine and configure it to use port forwarding on the local machine. Now, when you connect to the local port, it will redirect the traffic to the remote machine.

To secure communication between computers, SSH uses private and public encryption keys. The public encryption keys used by the SSH tunneling deed like the identifiers of the authorized computer. On initiating an SSH connection, each machine exchanges public keys, but only the computer that has the matching private key can attain access to the remote computer applications and information and can read encrypted communications with the public key.

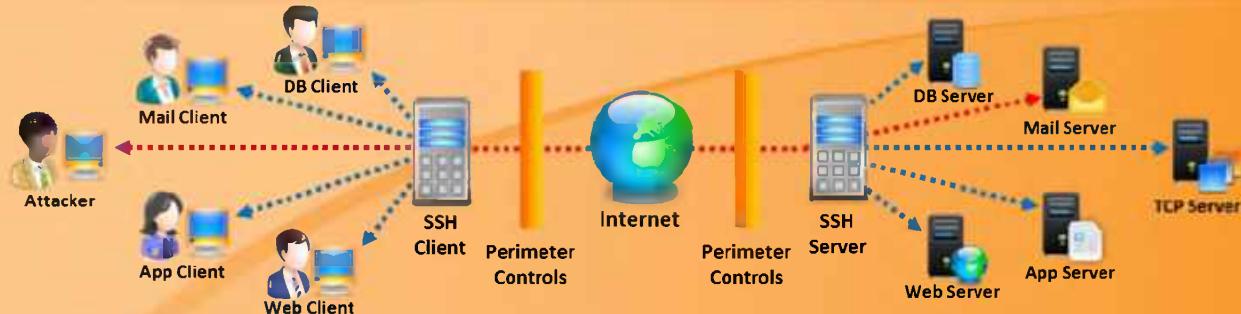


FIGURE 3.72: SSH Tunneling Process

OpenSSH

Source: <http://www.openssh.org>

OpenSSH encrypts all traffic (including passwords) to effectively eliminate eavesdropping, connection hijacking, and other attacks. Additionally, OpenSSH provides secure tunneling capabilities and several authentication methods, and supports all SSH protocol versions. OpenSSH can be used to tunnel the traffic on local machine to a remote machine that you have an account on.

```
ssh -f user@certifiedhacker.com -L 2000:certifiedhacker.com:25 -N
```

-f => background mode

user@certifiedhacker.com=> user name and server you are logging into

-L 2000:certifiedhacker.com:25 => local-port:host:remote-port

-N => Do not execute the command on the remote system

This essentially forwards the local port 2000 to port 25 on certifiedhacker.com encrypted. Simply point your email client to use localhost:2000 as the SMTP server.

SSH Tunneling Tool: Bitvise

- Bitvise SSH Server provides secure **remote login capabilities** to Windows workstations and servers
- SSH Client includes powerful tunneling features including **dynamic port forwarding** through an integrated proxy, and also **remote administration** for the SSH Server

http://www.bitvise.com

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



SSH Tunneling Tool: Bitvise

Source: <http://www.bitvise.com>

Bitvise is client **server-based application** used for SSH tunneling. The server provides you secure remote login capabilities to Windows workstations and servers. With Bitvise SSH Server, you can administer the **Windows server remotely**. The Bitvise server even has the ability to encrypt the data during transmission so that no one can sniff your data during transmission.

Bitvise SSH Client includes graphical as well as command line SFTP support, an FTP-to-SFTP bridge, tunneling features that can be helpful for port forwarding and remote administration.

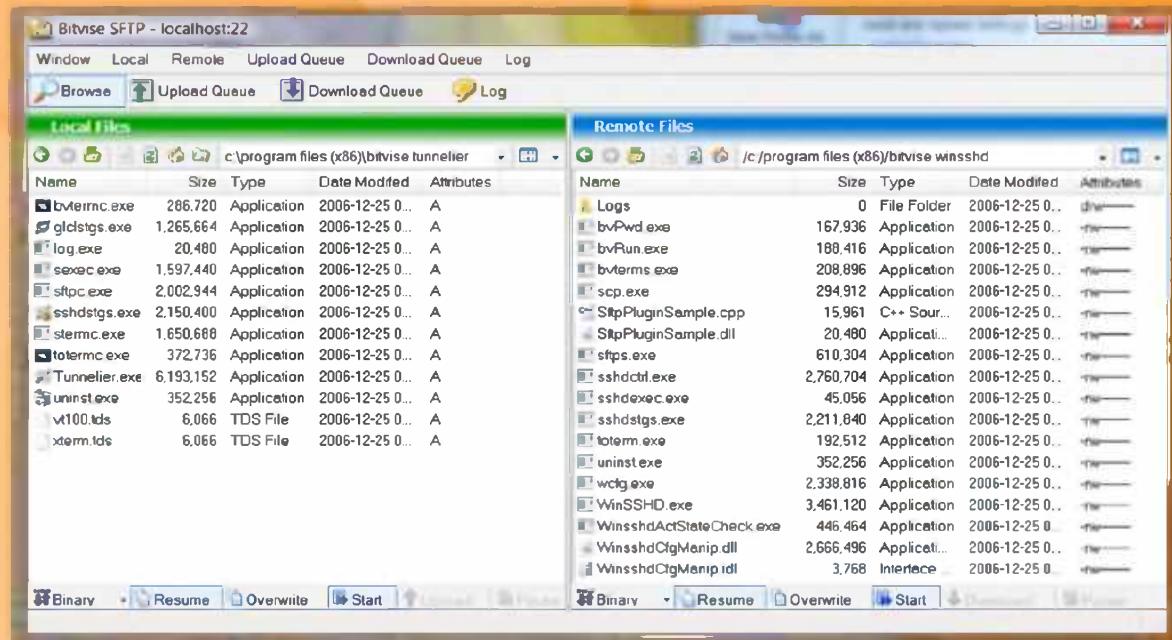


FIGURE 3.73: Bitvise Tool Screenshot

Anonymizers

C|EH
Certified Ethical Hacker

- An anonymizer removes all the identifying information from the user's computer while the user surfs the Internet
- Anonymizers make activity on the Internet untraceable
- Anonymizer tools allow you to bypass Internet censored websites



Why use Anonymizer?



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

Anonymizers

An anonymizer is an **intermediate server** placed in between the **end user** and **web site** that accesses the website on behalf of you, making your web surfing untraceable. An anonymizer eliminates all the identifying information (IP address) from your system while you are surfing the Internet, thereby ensuring privacy. Most anonymizers can anonymize the web (**http :)**, file transfer protocol (**ftp :)**, and gopher (**gopher :)** Internet services.

To visit a page anonymously, you can visit your preferred anonymizer site, and enter the name of the target website in the Anonymization field. Alternately, you can set your browser home page to point to an anonymizer, so that every subsequent web access will be anonymized. Apart from this, you can choose to anonymously provide passwords and other information to sites that request you, without revealing any other information, such as your IP address. Crackers may configure an anonymizer as a permanent proxy server by making the site name the setting for the HTTP, FTP, Gopher, and other proxy options in their applications configuration menu, thereby cloaking their malicious activities.



Why Use an Anonymizer?

The reasons for using anonymizers include:

- ⌚ **Ensures privacy:** It protects your identity by making your **web navigation** activities **untraceable**. Your privacy is maintained until and unless you disclose your personal information on the web by filling out forms, etc.
- ⌚ **Accesses government-restricted content:** Most governments prevent their citizens from accessing certain websites or content in order to avoid them from accessing inappropriate information or sensitive information. But these people can access even these types of resources by an anonymizer located outside the country.
- ⌚ **Protect you from online attacks:** Anonymizers protect you from all instances of online pharming attacks by routing all customer Internet traffic via the anonymizer's protected **DNS servers**.
- ⌚ **Bypass IDS and firewall rules:** Bypassing of firewalls is mostly done in organizations or schools by employees or students accessing websites they are not supposed to access. An anonymizer service gets around your organization's firewall by setting up a connection between your computer and the anonymizer service. By doing such, firewalls can see only the connection from you to anonymizer's web address. The anonymizer will then connect to Twitter or any website you wanted to access with the help of an Internet connection and sends the content back to you. For your organization, it looks like your system is connected to an anonymizer's web address, but not to Twitter or other sites.

Anonymizers, apart from protecting users' identities, can also attack the website and no one can actually detect where the attack came from.



Types of Anonymizers

An anonymizer is a service through which one can hide their identity when using certain services of the Internet. It basically works by encrypting the data from your computer, so that it cannot be understood by Internet service providers or anyone who might try to access it. Basically, anonymizers are of two types:

- ⌚ Networked anonymizers
- ⌚ Single-point anonymizers



Networked Anonymizers

These type of anonymizer first transfers your information through a network of Internet computers before sending it to the website. Since the information passes through several Internet computers, it becomes more cumbersome for anyone trying to track your information to establish the connection between you and anonymizer.

Example: If you want to visit any web page you have to make a request. The request will first pass through A, B, and C Internet computers prior to going to the website. Then after being opened, the page will be transferred back through C, B, and A and then to you.

Advantage: Complication of the communications makes **traffic analysis complex**

Disadvantage: Any multi-node network communications have some degree of risk at each node for compromising confidentiality



Single-point Anonymizers

Single-point anonymizers first transfer your information through a website before sending this to the target website, and then pass back information, i.e., gathered from the targeted website, through a website and then back to you to protect your identity.

Advantage: IP address and related identifying information are protected by the arms-length communications

Disadvantage: It offers less resistance to sophisticated traffic analysis

Case: Bloggers Write Text Backwards to Bypass Web Filters in China

The diagram features a central globe with dashed lines pointing to three main points:

- Top Left:** "Bloggers and journalists in China are using a novel approach to **bypass Internet filters** in their country – they write backwards or from right to left".
- Bottom Left:** "The content therefore remains readable by human beings but defeats the **web filtering software**".
- Bottom Right:** "China is implementing '**packet filtering**' to detect TCP packets containing controversial keywords such as Tibet, Democracy, Tiananmen, etc."

A red circle on the right contains the Chinese flag and the quote: "IF IT BOTHERS YOU THAT THE CHINA GOVERNMENT DOES IT, IT SHOULD BOTHER YOU WHEN YOUR CABLE COMPANY DOES IT."

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



Case: Bloggers Write Text Backwards to Bypass Web Filters in China

China is well known for its implementation of the “**packet filtering**” technique. This technique **detects TCP packets** that contain controversial keywords such as Tibet, Democracy, Tiananmen, etc. To bypass Internet filters and dodge the censors, bloggers and journalists in China are writing the text backwards or from right to left. By doing so, though the content is still in human readable form, the text is successful in defeating web filtering software. Bloggers and journalists use vertical text converter tools to write the text backwards or from right to left and vertically instead of horizontally.

Censorship Circumvention Tool: Psiphon

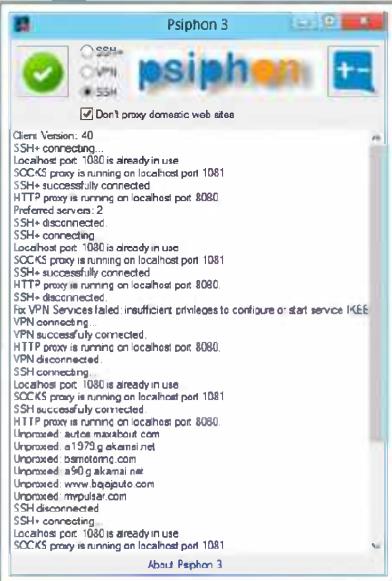
CEH Certified Ethical Hacker

- Psiphon is a censorship circumvention system that allows users to bypass firewalls and access blocked sites in countries where the Internet is censored
- It uses a secure, encrypted HTTP tunnel connection to receive requests from psiphonite to psiphonode which in turn transports the results back to the requested psiphonite
- It acts as a web proxy for authenticated psiphonites, even works on mobile devices
- It bypasses the content-filtering systems of countries like China, North Korea, Iran, Saudi Arabia, Egypt and others



<http://psiphon.ca>

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



Censorship Circumvention Tool: Psiphon

Source: <http://psiphon.ca>

Psiphon is a censorship circumvention system that allows users to bypass firewalls and access blocked sites in countries where the Internet is censored. It uses a secure, encrypted HTTP tunnel connection to receive requests from psiphonite to psiphonode, which in turn then transports the results back to the requested psiphonite. It acts as a web proxy for authenticated psiphonites, and works on mobile browsers. It bypasses content-filtering systems of countries such as China, North Korea, Iran, Saudi Arabia, Egypt, and others.

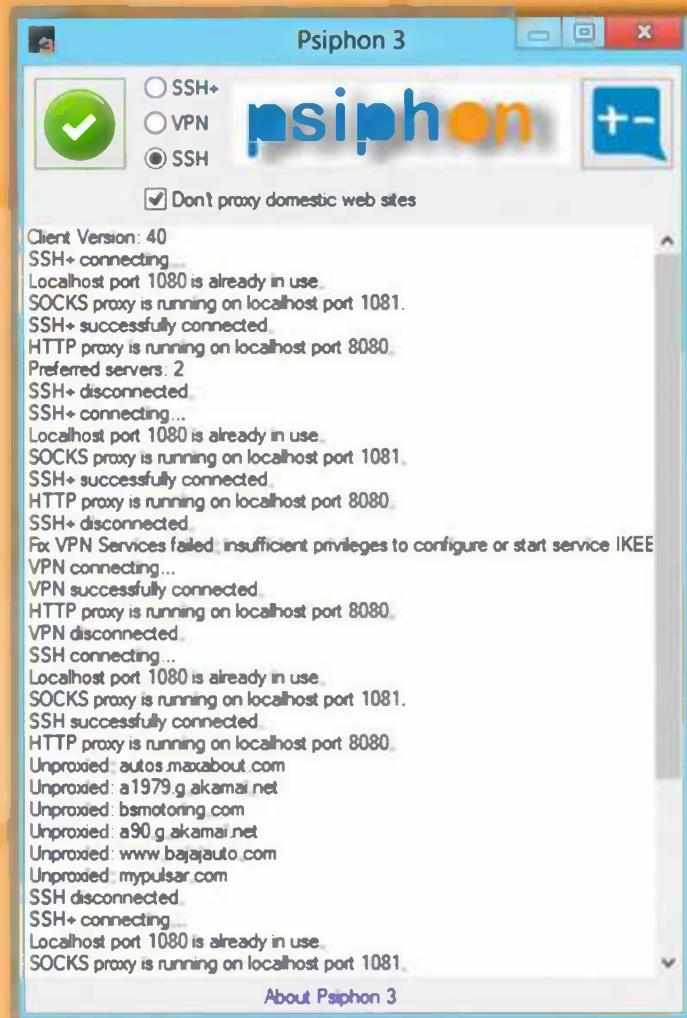


FIGURE 3.74: Psiphon Screenshot



Censorship Circumvention Tool: Your-Freedom

Source: <http://www.your-freedom.net>

Censorship circumvention tools allow you to **access websites** that are not accessible to you by **bypassing firewalls**. The Your Freedom services makes accessible what is unaccessible to you, and they hide your network address from those who don't need to know. This tool turns your PC into an uncensored, anonymous web proxy and an uncensored, anonymous **SOCKS proxy** that your applications can use, and if that's not enough, it can even get you connected to the Internet just as if you were using an unrestricted DSL or cable connection.

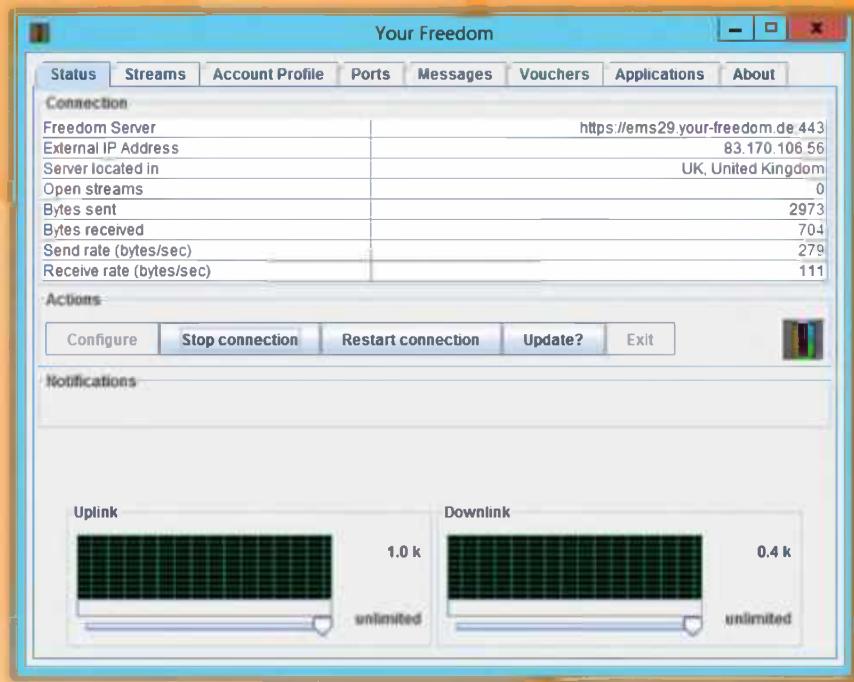


FIGURE 3.75: Your-Freedom Screenshot

How to Check if Your Website is Blocked in China or Not?

Internet tools help identify if web users in China can access remote websites
When Just Ping and WebSitePulse show "Packets lost" or "time-out" errors, chances are that the site is restricted

Just Ping

WebSitePulse

<http://www.just-ping.com>

<http://www.websitelpulse.com>

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



How to Check if Your Website is Blocked in China or Not?

"packets lost" error is received or there is a connection **time-out message** is displayed while connecting to your site, chances are that the site is blocked. To find out whether the website at xyz.com is accessible by Chinese web users, you can use tools such as just ping and WebSitePulse.



Just ping

Source: <http://www.just-ping.com>

Just ping is an online web-based ping tool that allows you to ping from various locations worldwide. It pings a website or IP address and displays the result as shown as follows:

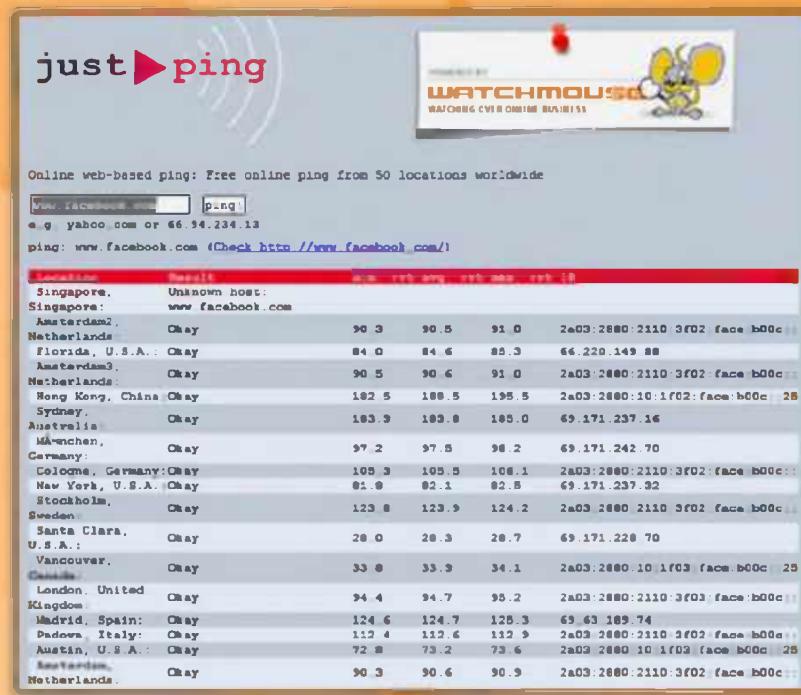


FIGURE 3.76: Just Ping Screenshot



WebsitePulse

Source: <http://www.websitepulse.com>

WebsitePulse provides remote monitoring services. It simultaneously pops websites from around the globe.

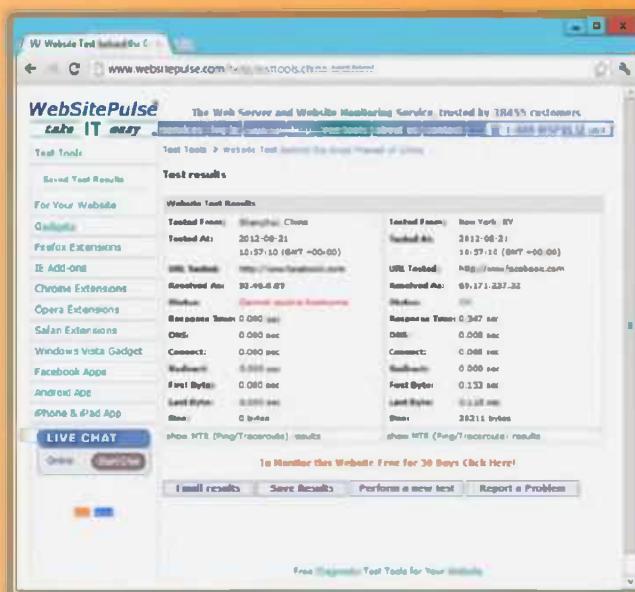
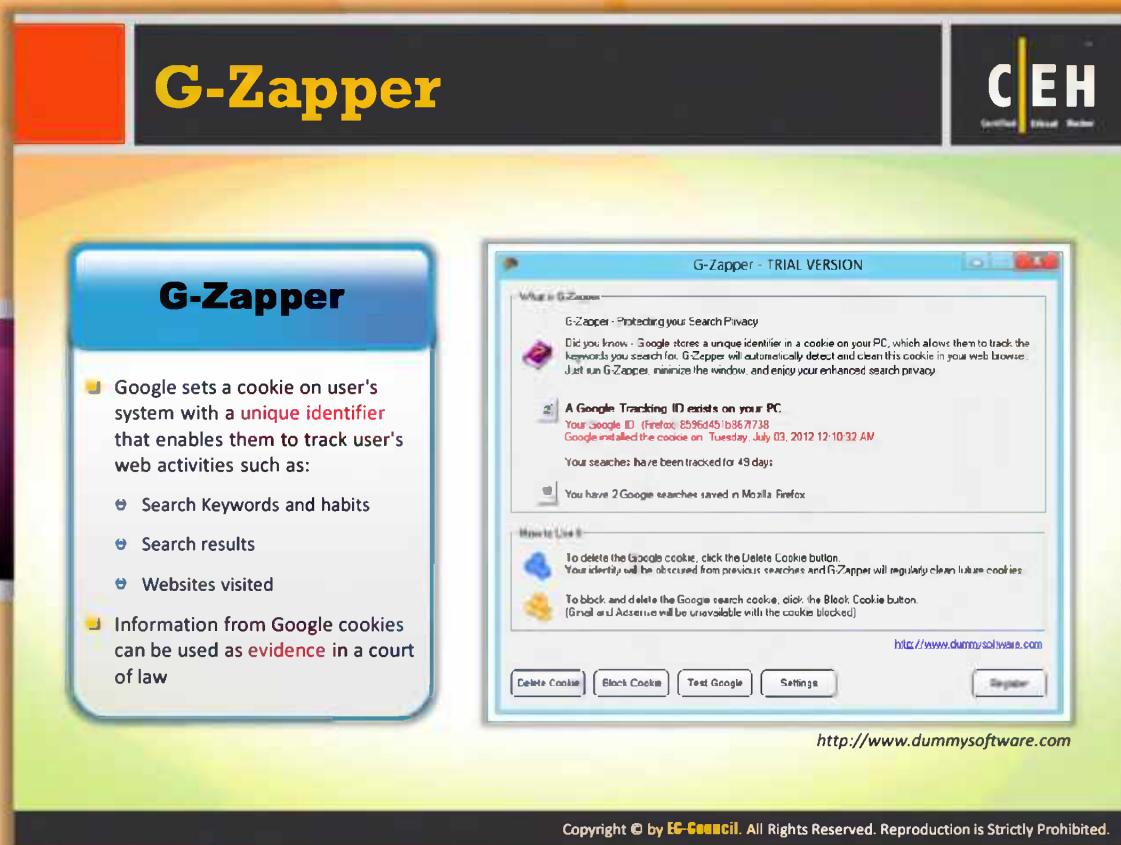


FIGURE 3.77: WebsitePulse Screenshot



G-Zapper

Source: <http://www.dummysoftware.com>

G-Zapper is a utility to **block Google cookies**, **clean Google cookies**, and help you stay anonymous while searching online. It automatically detects and cleans Google cookies each time you use your web browser.

It is compatible with **Windows 95/98/ME/NT/2000/XP/Vista/Windows7**. It requires Microsoft Internet Explorer, Mozilla Firefox, or Google Chrome and is compatible with Gmail, Adsense, and other Google services.



FIGURE 3.78: G-Zapper-Trial Version Screenshot

The slide has a yellow header bar with the title 'Anonymizers'. In the top right corner is the 'CEH' logo. Below the title, there are nine items, each with an icon and a link:

- Mowser (<http://www.mowser.com>)
- Spotflux (<http://www.spotflux.com>)
- Anonymous Web Surfing Tool (<http://www.anonymous-surfing.com>)
- U-Surf (<http://ultimate-anonymity.com>)
- Hide Your IP Address (<http://www.hideyouripaddress.net>)
- WarpProxy (<http://silent-surf.com>)
- Anonymizer Universal (<http://www.anonymizer.com>)
- Hope Proxy (<http://www.hopeproxy.com>)
- Guardster (<http://www.guardster.com>)
- Hide My IP (<http://www.privacy-pro.com>)

At the bottom of the slide, a copyright notice reads: 'Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.'

Anonymizers

An anonymizer is a tool that allows you to mask your IP address to visit websites without being tracked or identified, keeping your activity private. It allows you to access blocked content on the Internet with omitted advertisements. A few anonymizers that are readily available in the market are listed as follows:

- ⌚ Mowser available at <http://www.mowser.com>
- ⌚ Anonymous Web Surfing Tool available at <http://www.anonymous-surfing.com>
- ⌚ Hide Your IP Address available at <http://www.hideyouripaddress.net>
- ⌚ Anonymizer Universal available at <http://www.anonymizer.com>
- ⌚ Guardster available at <http://www.guardster.com>
- ⌚ Spotflux available at <http://www.spotflux.com>
- ⌚ U-Surf available at <http://ultimate-anonymity.com>
- ⌚ WarpProxy available at <http://silent-surf.com>
- ⌚ Hope Proxy available at <http://www.hopeproxy.com>
- ⌚ Hide My IP available at <http://www.privacy-pro.com>

Spoofing IP Address

C|EH
Certified Ethical Hacker

- IP spoofing refers to the procedure of an attacker changing his or her IP address so that he or she appears to be someone else
- When the victim replies to the address, it goes back to the spoofed address and not to the attacker's real address

IP spoofing using Hping2:
`Hping2 www.cretifiedhacker.com -a 7.7.7.7`

You will not be able to complete the three-way handshake and open a successful TCP connection by spoofing an IP address

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



Spoofing IP Addresses

Spoofing IP addresses enables attacks like hijacking. When spoofing, an attacker uses a fake IP in place of the attacker's assigned IP. When the attacker sends a connection request to the target host, the target host replies to the attacker's request. But the reply is sent to the spoofed address. When spoofing an address that doesn't exist, the target replies to a nonexistent system and then hangs until the session times out, consuming target resources.

IP spoofing using Hping2:

`Hping2 www.cretifiedhacker.com -a 7.7.7.7`

Using Hping2 you can perform IP spoofing. It helps you to send arbitrary **TCP/IP** packets to network hosts.

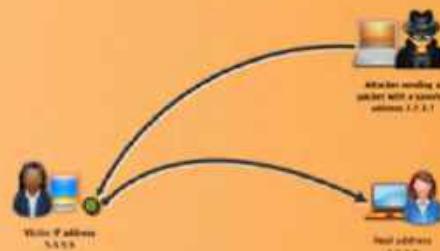


FIGURE 3.79: Attacker Sending Spoofed Packet to The Victim

IP Spoofing Detection Techniques: Direct TTL Probes

C|EH
Certified Ethical Hacker

The diagram shows an Attacker (laptop) sending a packet with a spoofed IP address (10.0.0.5) and a TTL of 13 to a Target (laptop). The Target replies with its own IP address (10.0.0.5) and a TTL of 25. A note at the bottom states: "Note: Normal traffic from one host can vary TTLs depending on traffic patterns".

Note: Normal traffic from one host can vary TTLs depending on traffic patterns

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



IP Spoofing Detection Techniques: Direct TTL Probes

Initially send a packet to the host of suspect spoofed packet and wait for the reply. Check whether the TTL value in the reply matches with the TTL value of the packet that you are checking. Both will have the same TTL if they are the same protocol. Though, initial **TTL values vary** based on the protocol used, a few initial TTL values are commonly used. For TCP/UDP, the commonly used initial values are **64** and **128** and for ICMP, the values are **128** and **255**. If the reply is from a different protocol, then you should check the actual hop count to detect the spoofed packets. The hop count can be determined by deducting the TTL value in the reply from the initial TTL value. If the TTL in the reply is not matching with the TTL of the packet that you are checking, it is a spoofed packet. If the attacker knows the hop count between source and host, it will be very easy for the attacker to launch an attack. In this case, the test results in a **false negative**.

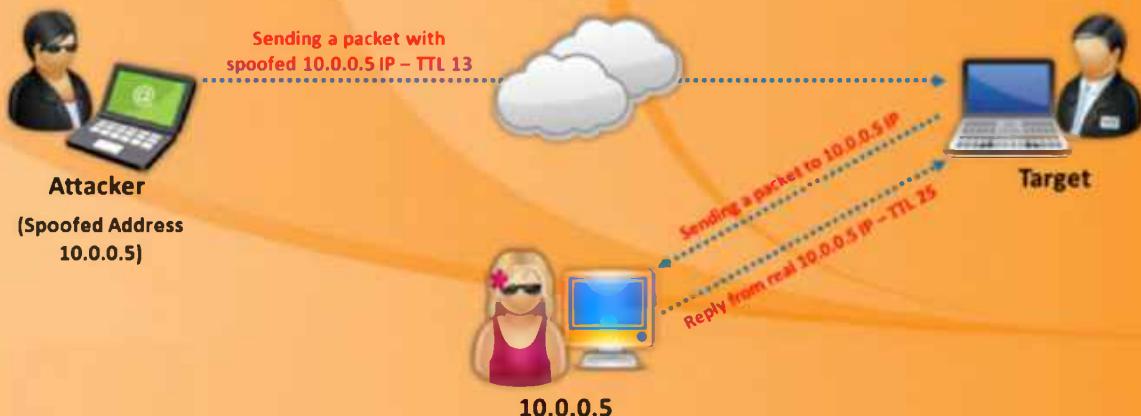


FIGURE 3.80: Using Direct TTL Probes for IP Spoofing Detection

IP Spoofing Detection Techniques: IP Identification Number

C|EH
Certified Ethical Hacker

- Send probe to host of suspect spoofed traffic that triggers reply and compare IP ID with suspect traffic
- If IP IDs are not in the near value of packet being checked, suspect traffic is spoofed
- This technique is successful even if the attacker is in the same subnet

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

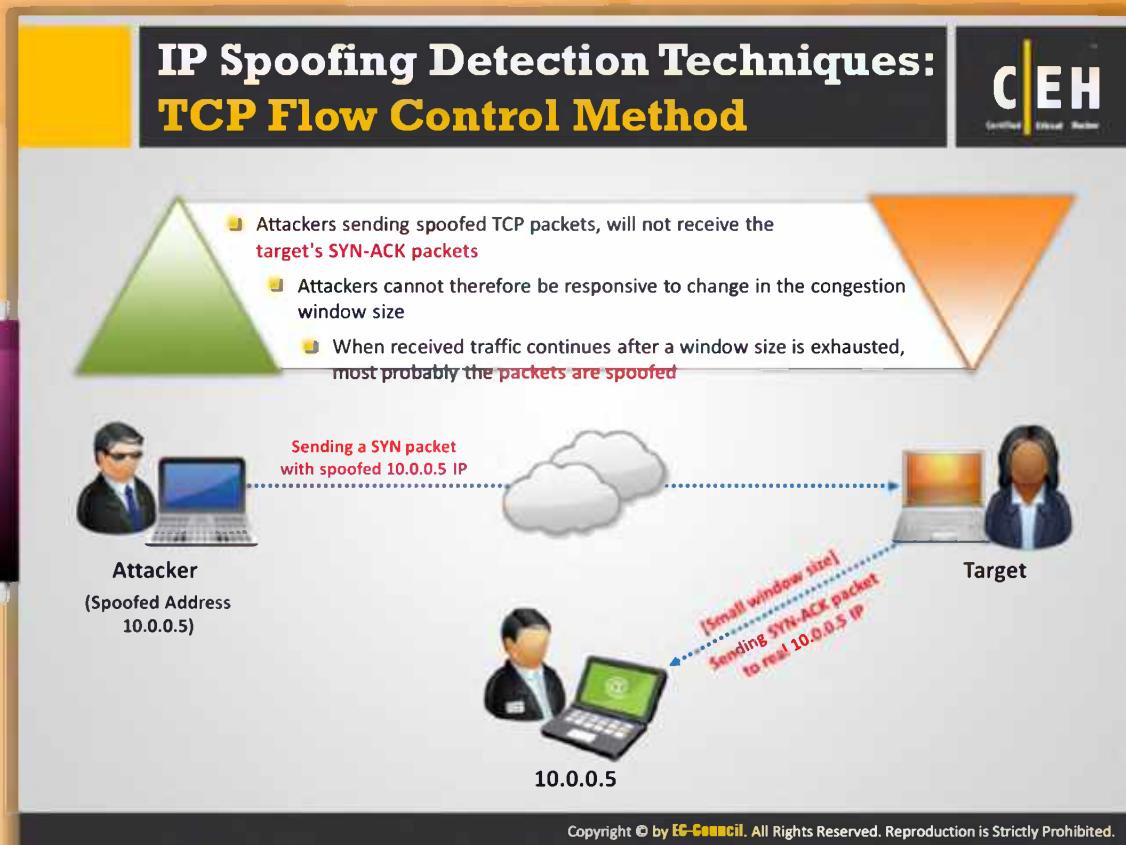
IP Spoofing Detection Techniques: IP Identification Number

Spoofed packets can be identified based on the identification number (IP ID) in the IP header that increases each time a packet is sent. This method is effective even when both the attacker and victim are on same subnet.

To identify whether the packet is spoofed or not, send a probe packet to the target and observe the IP ID number in the reply. If it is in the near value as the packet that you are checking, then it is not a spoofed packet, otherwise it is a spoofed packet.



FIGURE 3.81: Using IP Identification Number for IP Spoofing Detection



IP Spoofing Detection Techniques: TCP Flow Control Method

The TCP can optimize the **flow control** on both the **send** and the **receiver side** with its algorithm. The algorithm accomplishes the flow control based on the sliding window principle. The flow of IP packets can be **controlled by the window size** field in the **TCP header**. This field represents the maximum amount of data that the recipient can receive and the maximum amount of data the sender can transmit without acknowledgement. Thus, this field helps us to control data flow. When the window size is set to **zero**, the sender should stop sending more data.

In general flow control, the sender should stop sending data once the initial window size is exhausted. The attacker who is unaware of the **ACK packet containing window size information** continues to send data to the victim. If the victim receives data packets beyond the window size, then the packets must be treated as spoofed. For effective flow control method and early detection of spoofing, the initial window size must be very small.

Most spoofing attacks occur during the handshake, as it is difficult to build multiple spoofing replies with the correct sequence number. Therefore, the flow control spoofed packet detection must be applied at the handshake. In a TCP handshake, the host sending the initial SYN packet waits for SYN-ACK before sending the ACK packet. To check whether you are getting

the SYN request from a genuine client or a spoofed one, you should set the SYN-ACK to zero. If the sender sends an **ACK** with any data, then it means that the sender is the spoofed one. This is because when the **SYN-ACK** is set to zero, the sender must respond to it only with the ACK packet but not ACK with data.



FIGURE 3.82: Using TCP Flow Control Method for IP Spoofing Detection

IP Spoofing Countermeasures

Limit access to configuration information on a machine	Do not rely on IP-based authentication
Use random initial sequence numbers	Strictly filter use of ICMP
Ingress Filtering - Use router filters to prevent packets from entering your network	Reduce TTLs in TCP/IP requests
Egress Filtering - Use filters to prevent packets from leaving your network	Block private or unauthorized IP addresses using access control lists
Encrypt all network traffic	Use multiple firewalls providing multi-layered depth of protection

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



IP Spoofing Countermeasures

In ethical hacking, the ethical hacker also known as the **pen tester**, has to perform an additional task that a normal hacker doesn't follow, i.e., applying countermeasures to the respective vulnerabilities determined through hacking. This is essential because knowing security loopholes in your network is worthless unless you take measures to protect them **against real hackers**. As mentioned previously, IP spoofing is one of the techniques that a hacker employs to break into the target network. Therefore, in order to protect your network from external hackers, you should apply IP spoofing countermeasures to your network security settings. The following are a few IP spoofing countermeasures that you can apply:

Avoid trust relationships

Attackers may spoof themselves as a trusted host and send **malicious packets** to you. If you accept those packets by considering that the packets are sent by your trusted host, then you may get infected. Therefore, it is advisable to test the packets even when they come from one of your trusted hosts. You can avoid this problem by **implementing password authentication** along with **trust-relationship-based authentication**.

Use firewalls and filtering mechanisms

You should filter all the incoming and outgoing packets to avoid attacks and sensitive information loss. The incoming packets may be the malicious packets coming from the attacker.

If you do not employ any kind of incoming packet filtering mechanism such as a firewall, then the malicious packets may enter your private network and may cause severe loss. You can use access control lists (ACLs) to **block unauthorized access**. At the same time, there is also a possibility of insider attackers. These attackers may send sensitive information about your business to your competitors. This may also lead to great monetary loss or other issues. There is one more risk of outgoing packets, which is when an attacker succeeds in installing a malicious sniffing program running in hidden mode on your network. These programs gather and send all your network information to the attacker without giving any notification. This can be figured out by filtering the outgoing packets. Therefore, you should give the same importance to the scanning of outgoing packets as that of the incoming packet data scanning.

Use random initial sequence numbers

Most of the devices chose their ISN based on timed counters. This makes the ISNs predictable as it is easy for a malicious person to determine the concept of generating the ISN. An attacker can determine the ISN of the next **TCP connection** by analyzing the ISN of the current session or connection. If the attacker can predict the ISN, then he or she can make a malicious connection to the server and sniff your network traffic. To avoid this, risk you should use random initial sequence numbers.

Ingress filtering

Prohibiting spoofed traffic from entering the Internet is the best way to block it. This can be achieved with the help of ingress filtering. Ingress filtering applied on routers enhances the functionality of the routers and blocks spoofed traffic. It can be implemented in many ways. Configuring and using **access control lists (ACLs)** that drop packets with source address outside the defined range is one way to implement ingress filtering.

Egress filtering

Egress filtering refers to a practice that aims at **IP spoofing** prevention by blocking the outgoing packets with a source address that is not inside.

Use encryption

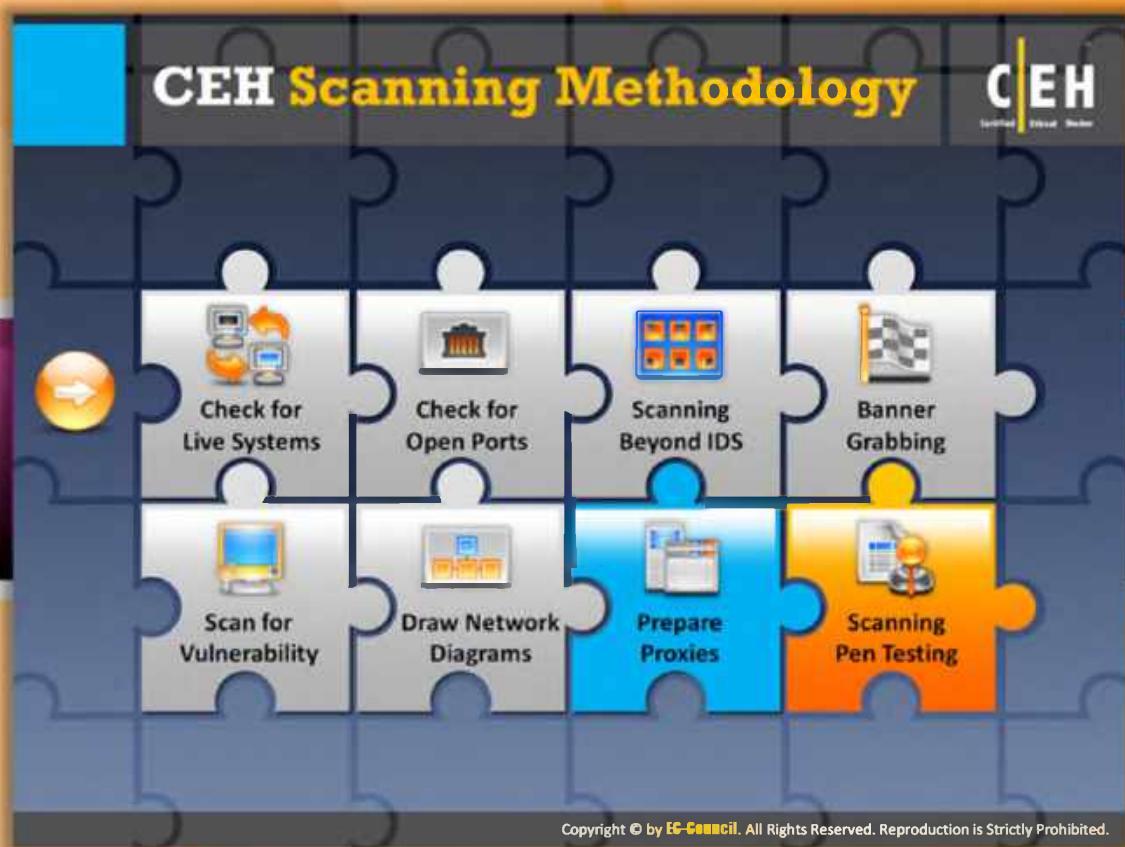
If you want to attain maximum network security, then use **strong encryption** for all the traffic placed onto the transmission media without considering its type and location. This is the best solution for IP spoofing attacks. Attackers usually tend to find targets that can be compromised easily. If an attacker wants to break into encrypted network, then he or she has to face a whole slew of encrypted packets, which is a difficult task. Therefore, the attacker may try to find another target that can be easily compromised or may attempt other techniques to break into the network. Use the latest encryption algorithms that provide strong security.

SYN flooding countermeasures

Countermeasures against SYN flooding attacks can also help you to avoid IP spoofing attacks.

Besides these basic countermeasures, you can perform the following to avoid IP spoofing attacks:

- ⊕ You should limit the access to configuration information on a machine
- ⊕ You should always disable commands like **ping**
- ⊕ You should reduce **TTL fields** in TCP/IP requests
- ⊕ You should use multilayered firewalls



CEH Scanning Methodology

So far, we have discussed concepts such as what to scan, how to scan, how to detect vulnerabilities, and the respective countermeasures that are necessary to perform scanning pen testing. Now we will begin the action of **scanning pen testing**.

 Check for Live Systems	 Scan for Vulnerability
 Check for Open Ports	 Draw Network Diagrams
 Scanning Beyond IDS	 Prepare Proxies
 Banner Grabbing	 Scanning Pen Testing

This section highlights the need to scan pen testing and the steps to be followed for effective pen testing.

Scanning Pen Testing

C|EH
Certified Ethical Hacker

- Pen testing a network for scanning vulnerabilities determines the network's **security posture** by identifying **live systems**, discovering **open ports**, associating **services** and grabbing system banners to simulate a network hacking attempt
- The penetration testing report will help **system administrators** to:

Close **unused ports**

Disable **unnecessary services**

Hide or customize banners

Troubleshoot service configuration errors

Calibrate firewall rules

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

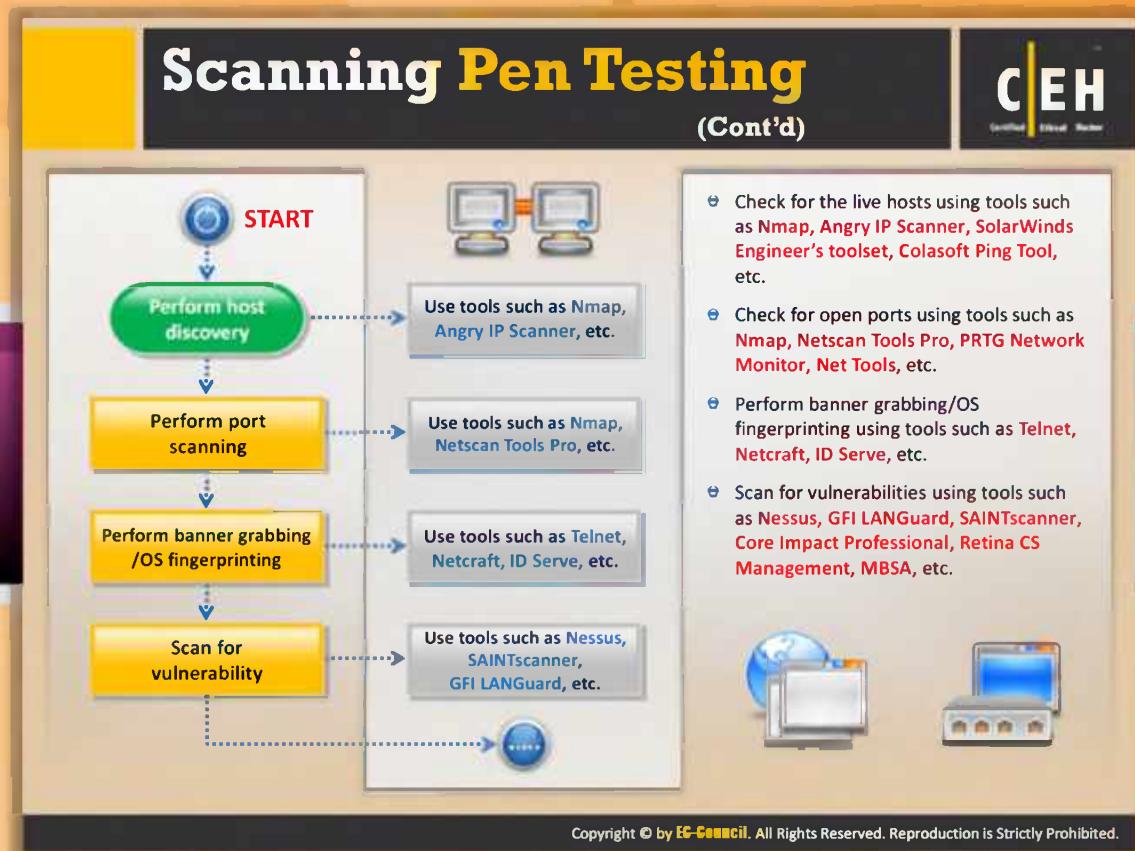


Scanning Pen Testing

The network scanning penetration test helps you to determine the **network security posture** by identifying live systems, discovering open ports and associated services, and grabbing system banners from a remote location, simulating a **network hacking attempt**. You should scan or test the network in all possible ways to ensure that no security loophole is overlooked.

Once you are done with the penetration testing, you should **document** all the **findings** obtained at every stage of testing so that it helps system administrators to:

- Close **unused ports** if not necessary/unknown open ports found
- Disable unnecessary **services**
- Hide or customize banners**
- Troubleshoot service configuration errors**
- Calibrate firewall rules** to impose more restriction



Scanning Pen Testing (Cont'd)

Let's see step by step how a penetration test is conducted on the target network.

Step 1: Host Discovery

The first step of network penetration testing is to **detect live hosts** on the target network. You can attempt to detect the live host, i.e., **accessible hosts** in the target network, using **network scanning tools** such as **Angry IP Scanner**, **Nmap**, **Netscan**, etc. It is difficult to detect live hosts behind the firewall.

Step 2: Port Scanning

Perform port scanning using tools such as **Nmap**, **Netscan Tools Pro**, **PRTG Network Monitor**, **Net Tools**, etc. These tools will help you to probe a server or host on the target network for open ports. **Open ports** are the **doorways** for attackers to install **malware** on a system. Therefore, you should check for open ports and close them if not necessary.

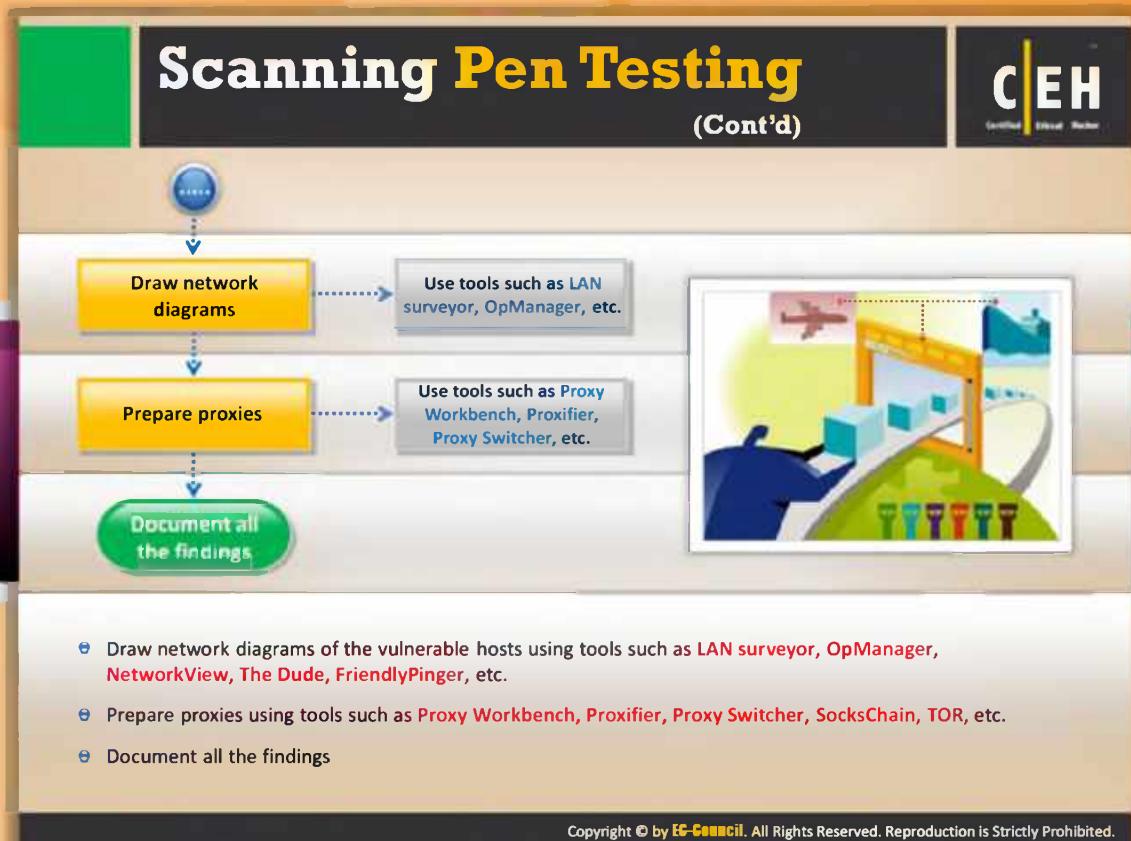
Step 3: Banner Grabbing or OS Finger Printing

Perform banner **grabbing/OS** fingerprinting using tools such as Telnet, Netcraft, ID Serve, Netcat, etc. This determines the **operating system** running on the target host of a network and its **version**. Once you know the version and operating system running on the target system, find

and exploit the **vulnerabilities** related to that OS. Try to **gain control** over the system and compromise the whole network.

Step 4: Scan for Vulnerabilities

Scan the network for vulnerabilities using **network vulnerability scanning tools** such as **Nessus**, **GFI LANGuard**, **SAINT**, **Core Impact Professional**, **Ratina CS**, **MBSA**, etc. These tools help you to find the vulnerabilities present in the target network. In this step, you will be able to determine the **security weaknesses/loopholes** of the target system or network.



Scanning Pen Testing (Cont'd)

Step 5: Draw Network Diagrams

Draw a network diagram of the target organization that helps you to understand the **logical connection** and **path** to the **target host** in the network. The network diagram can be drawn with the help of tools such as **LAN surveyor**, **OpManager**, **LANState**, **FriendlyPinger**, etc. The network diagrams provide valuable information about the network and its architecture.

Step 6: Prepare Proxies

Prepare proxies using tools such as Proxifier, SocksChain, SSL Proxy, Proxy+, Gproxy, ProxyFinder, etc. to hide yourself from being caught.

Step 7: Document all Findings

The last but the most important step in **scanning penetration testing** is **preserving** all outcomes of tests conducted in previous steps in a document. This document will assist you in finding **potential vulnerabilities** in your network. Once you determine the potential vulnerabilities, you can plan the **counteractions** accordingly. Thus, penetration testing helps in assessing your network before it gets into real trouble that may cause severe loss in terms of value and finance.

Module Summary



- The objective of scanning is to discover live systems, active/running ports, the operating systems, and the services running on the network
- Attacker determines the live hosts from a range of IP addresses by sending ICMP ECHO requests to multiple hosts
- Attackers use various scanning techniques to bypass firewall rules and logging mechanism, and hide themselves as usual network traffic
- Banner grabbing or OS fingerprinting is the method to determine the operating system running on a remote target system
- Drawing target's network diagram gives valuable information about the network and its architecture to an attacker
- HTTP Tunneling technology allows users to perform various Internet tasks despite the restrictions imposed by firewalls
- Proxy is a network computer that can serve as an intermediary for connecting with other computers
- A chain of proxies can be created to evade a traceback to the attacker

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



Module Summary

Let's take a look at what you have learned in this module:

- ☐ The objective of scanning is to **discover live systems, active/running ports, the operating systems, and the services** running on the network.
- ☐ Attacker determines the live hosts from a range of IP addresses by sending **ICMP ECHO requests** to multiple hosts.
- ☐ Attackers use various scanning techniques to bypass firewall rules, logging mechanism, and hide themselves as usual network traffic.
- ☐ **Banner Grabbing or OS fingerprinting** is the method to determine the operating system running on a remote target system.
- ☐ Drawing target's network diagram gives valuable information about the network and its **architecture** to an attacker.
- ☐ **HTTP Tunneling** technology allows users to perform various Internet tasks despite the restrictions imposed by firewalls.
- ☐ **Proxy** is a network computer that can serve as an intermediary for connecting with other computers.
- ☐ A chain of proxies can be created to evade a traceback to the attacker.