CEH: Understanding Ethical Hacking

Eng.\ Mohamed Magdy Ali
Cyber Security Specialist

Agenda

- What is **Hacking**?
- Who is a **Hacker**?
- What is **Ethical Hacking**?
- Why **Ethical Hacking** is Necessary?
- Why should I care?
- The Phases of Ethical Hacking
- Network vs Web Browser Attacks
- Who is Responsible for my Data in the Cloud
- Vulnerability Assessments & Penetration Testing
- What is in the Course

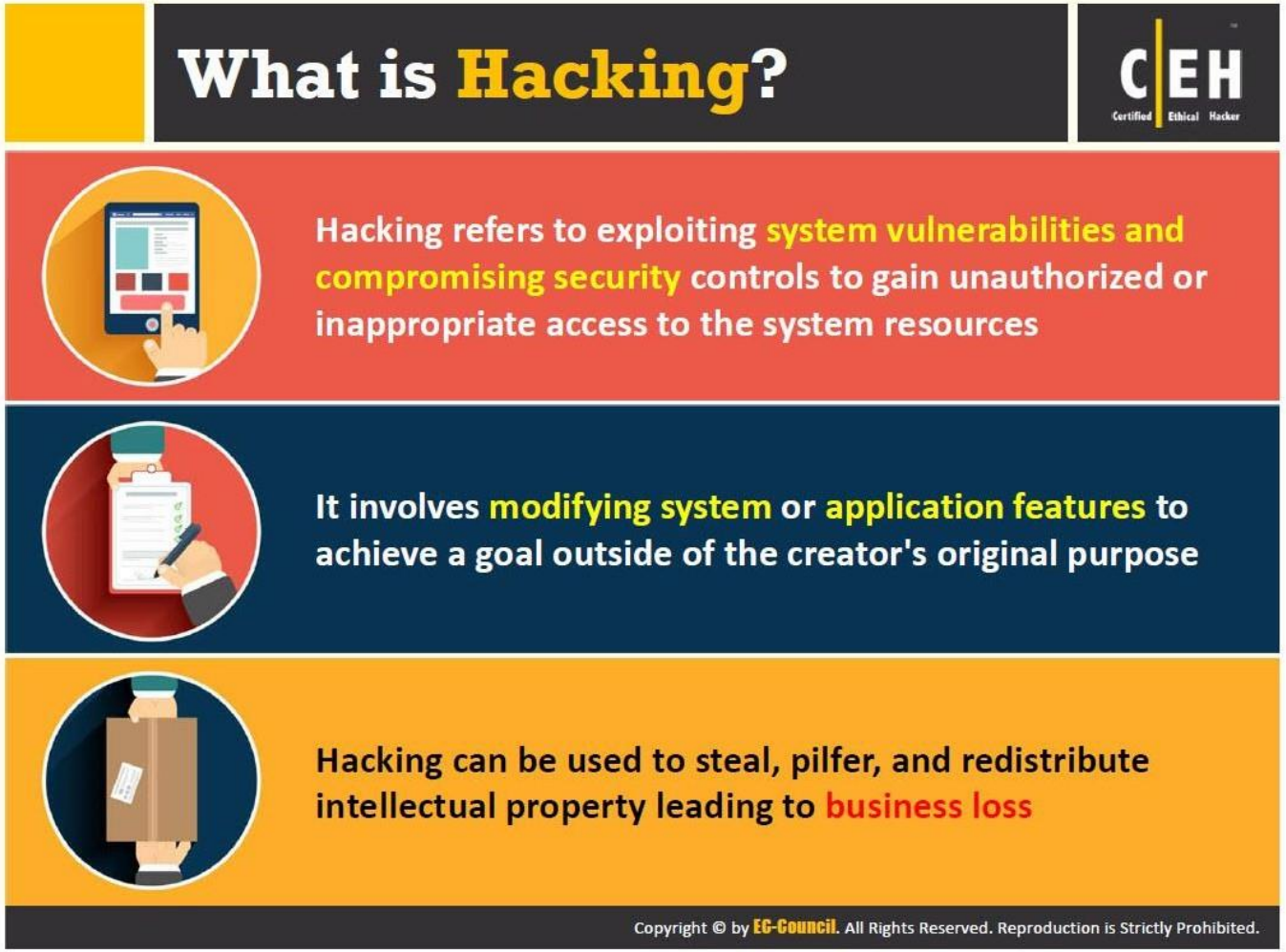
Think Like a Hacker

RFC 2828 Internet Security Glossary May 2000

$ hacker
(I) Someone with a strong interest in computers, who enjoys learning about them and experimenting with them. (See: cracker.)

(C) The recommended definition is the original meaning of the term (circa 1960), which then had a neutral or positive connotation of "someone who figures things out and makes something cool happen". Today, the term is frequently misused, especially by journalists, to have the pejorative meaning of cracker.

What is Hacking?



Who is a Hacker?

What is Ethical Hacking?

What is Ethical Hacking?

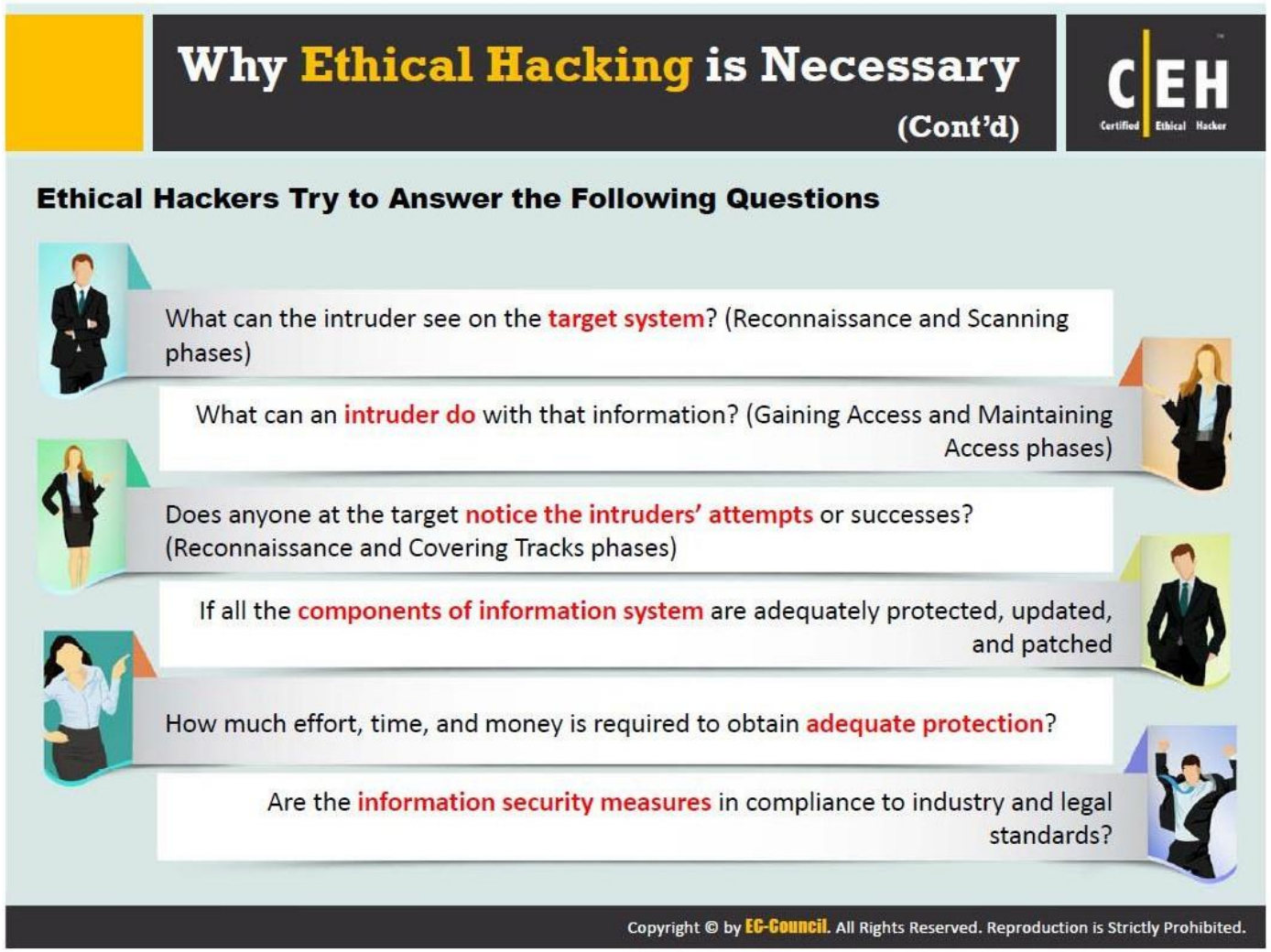
Ethical hacking involves the use of hacking tools, tricks, and techniques to **identify vulnerabilities** so as to ensure system security

It focuses on simulating techniques used by attackers to **verify the existence of exploitable vulnerabilities** in the system security

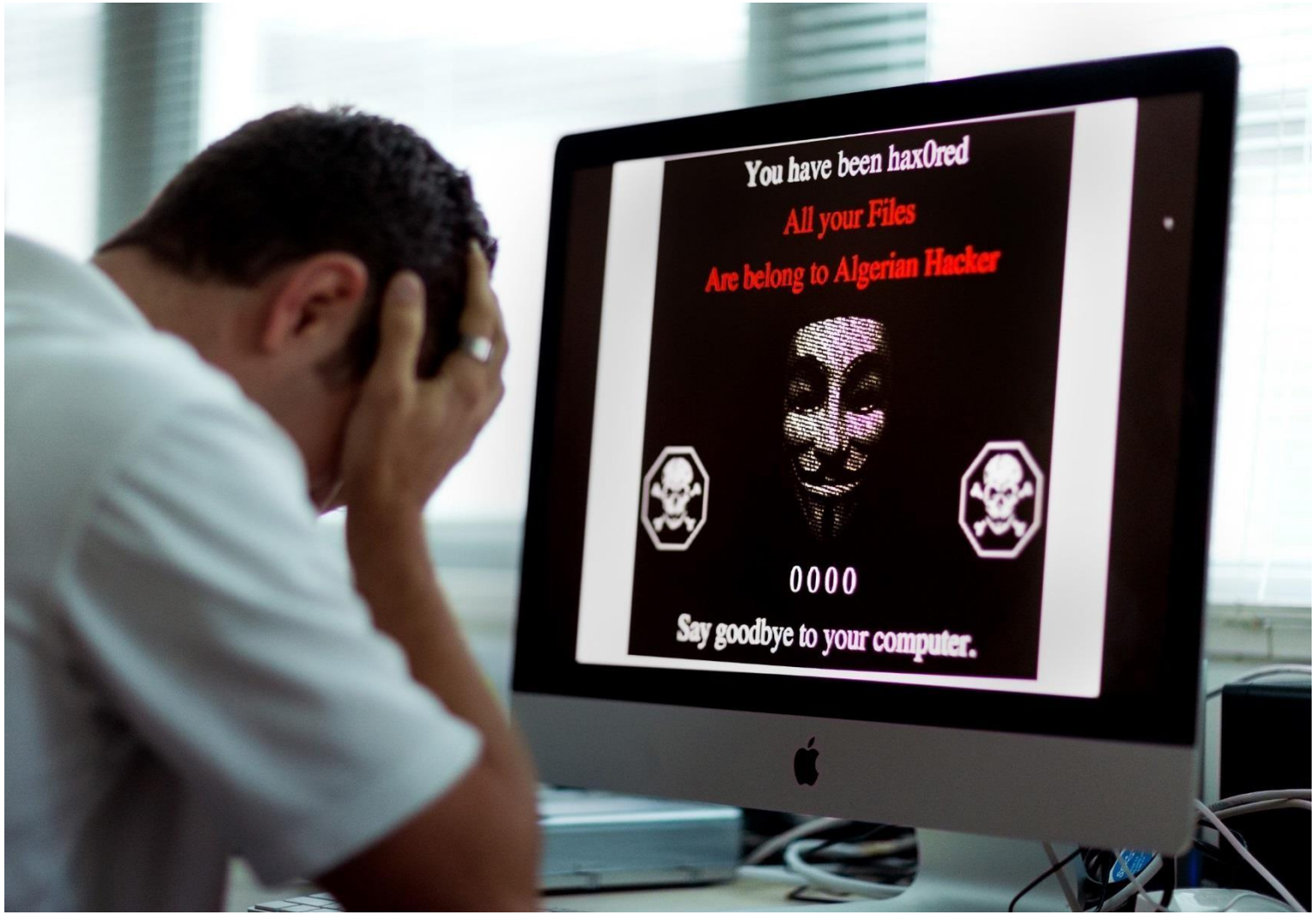
Ethical hackers performs security assessment of their organization **with the permission of concerned authorities**

Why Ethical Hacking is Necessary?

Why Ethical Hacking is Necessary?

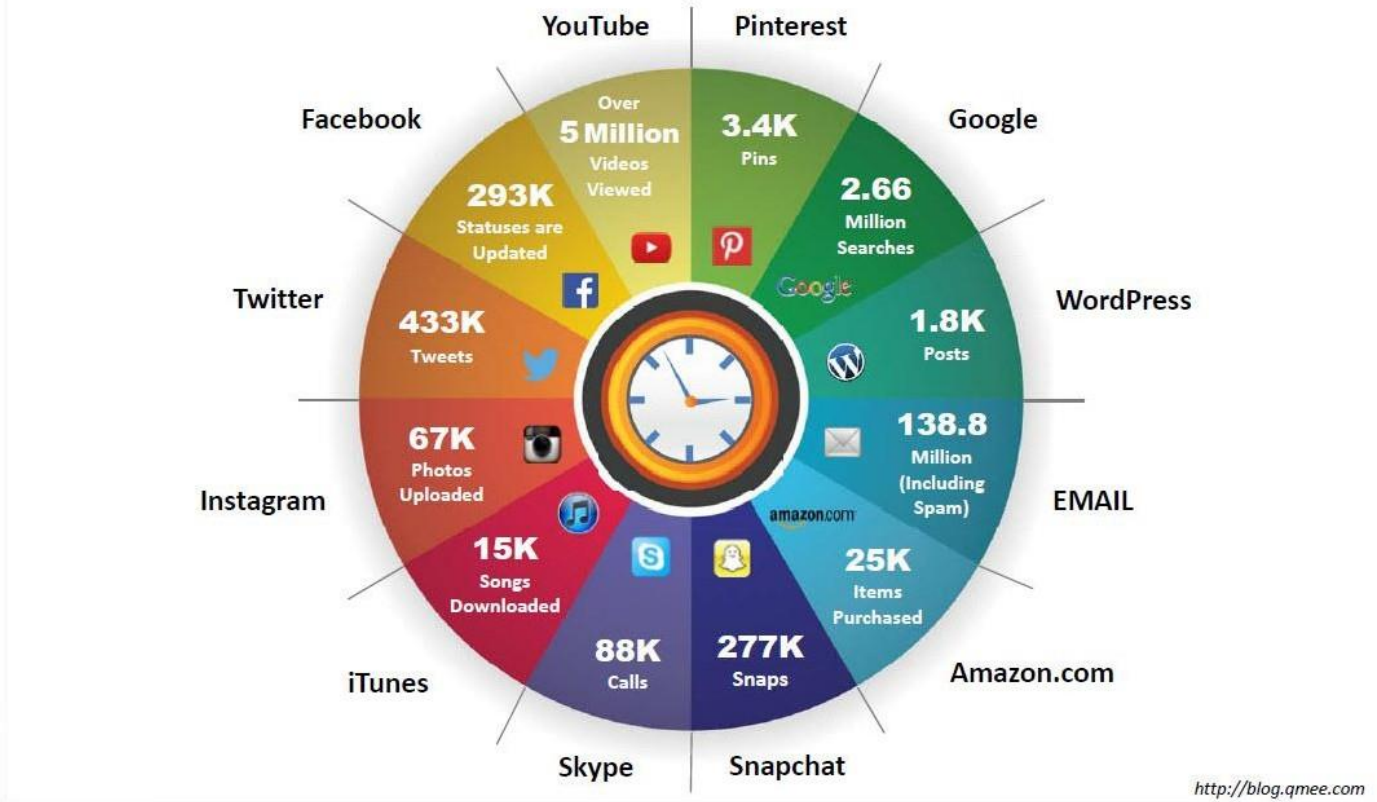


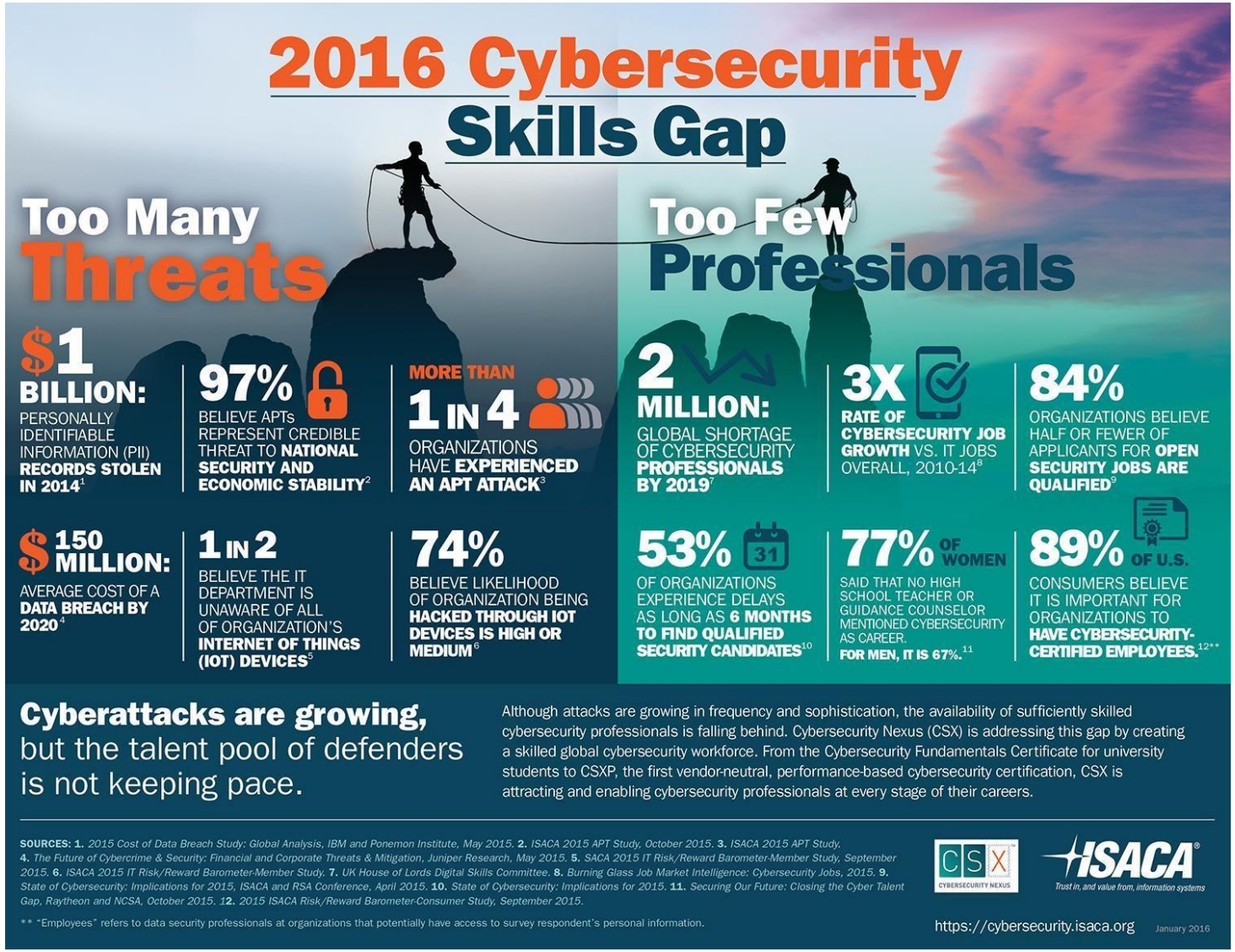
Why Should I Care



Internet is Integral Part of Business and Personal Life

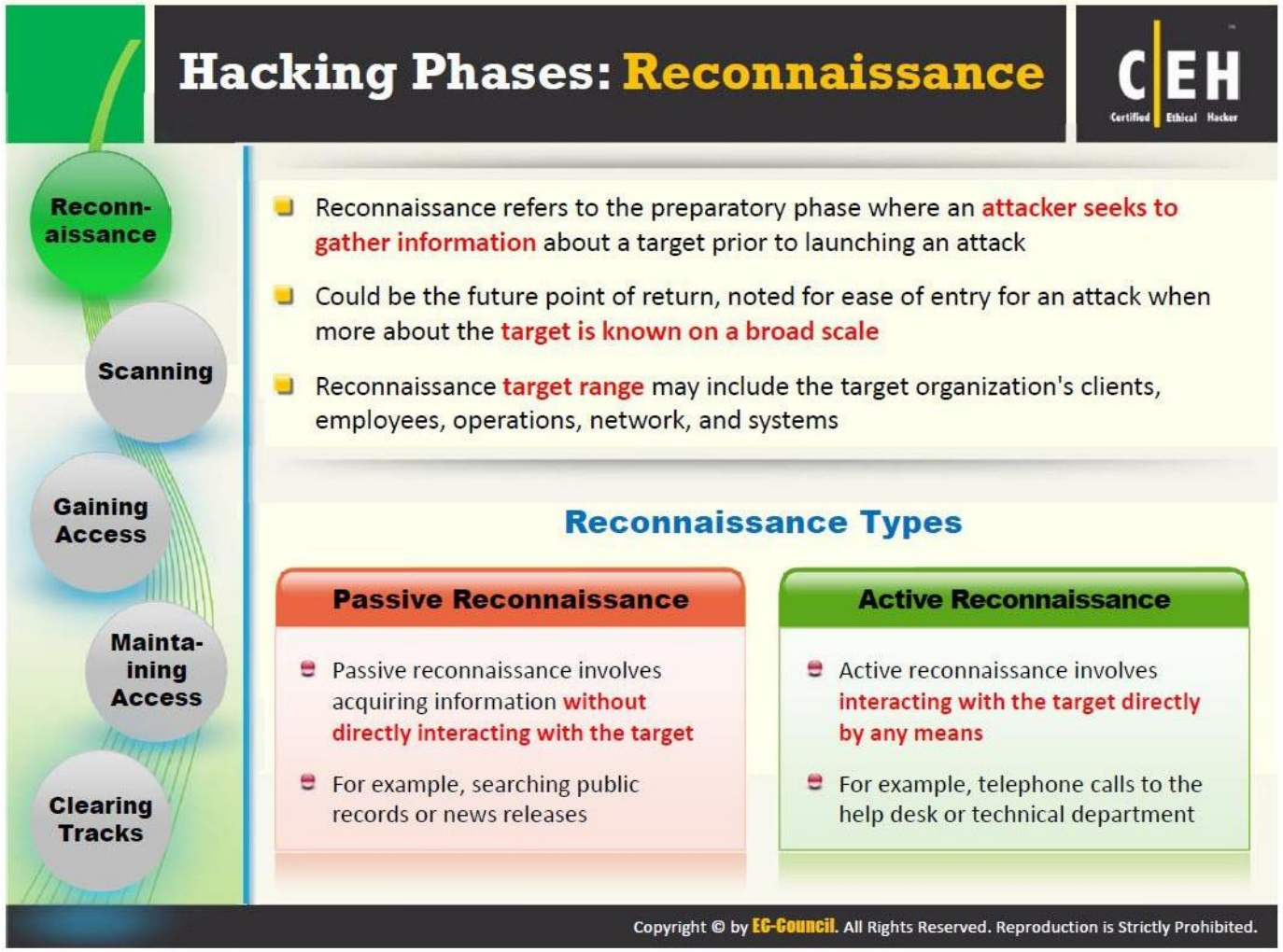
- What Happens Online in 60 Seconds



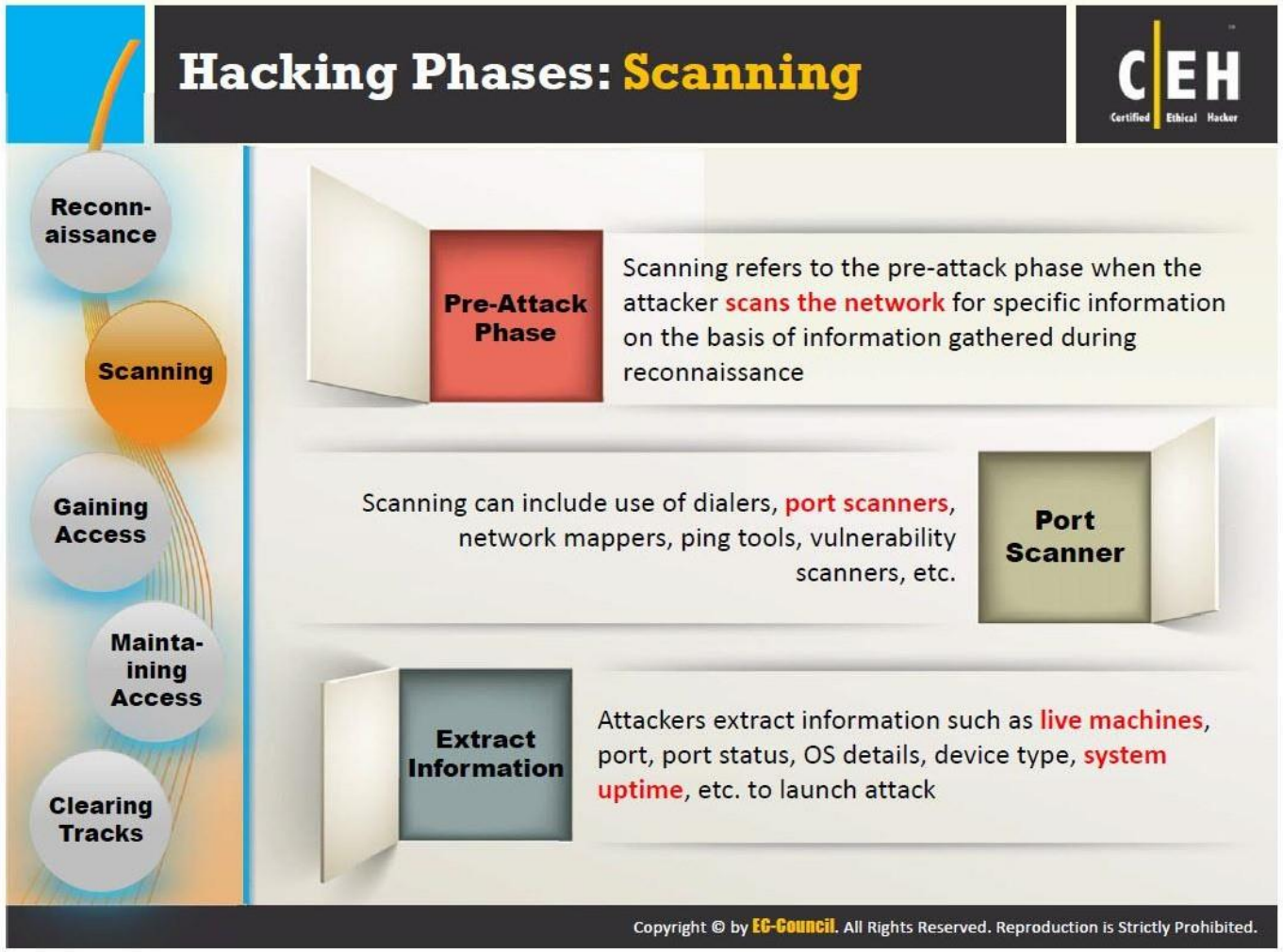

2016 Cybersecurity Skills Gap
Too Many Threats
$1 BILLION: PERSONALLY IDENTIFIABLE INFORMATION (PII) RECORDS STOLEN IN 2014[1]
97% BELIEVE APTs REPRESENT CREDIBLE THREAT TO NATIONAL SECURITY AND ECONOMIC STABILITY[2]
MORE THAN 1 IN 4 ORGANIZATIONS HAVE EXPERIENCED AN APT ATTACK[3]
$150 MILLION: AVERAGE COST OF A DATA BREACH BY 2020[4]
1 IN 2 BELIEVE THE IT DEPARTMENT IS UNAWARE OF ALL OF ORGANIZATION'S INTERNET OF THINGS (IOT) DEVICES[5]
74% BELIEVE LIKELIHOOD OF ORGANIZATION BEING HACKED THROUGH IOT DEVICES IS HIGH OR MEDIUM[6]
Too Few Professionals
2 MILLION: GLOBAL SHORTAGE OF CYBERSECURITY PROFESSIONALS BY 2019[7]
3X RATE OF CYBERSECURITY JOB GROWTH VS. IT JOBS OVERALL, 2010-14[8]
84% ORGANIZATIONS BELIEVE HALF OR FEWER OF APPLICANTS FOR OPEN SECURITY JOBS ARE QUALIFIED[9]
53% OF ORGANIZATIONS EXPERIENCE DELAYS AS LONG AS 6 MONTHS TO FIND QUALIFIED SECURITY CANDIDATES[10]
77% OF WOMEN SAID THAT NO HIGH SCHOOL TEACHER OR GUIDANCE COUNSELOR MENTIONED CYBERSECURITY AS CAREER. FOR MEN, IT IS 67%.[11]
89% OF U.S. CONSUMERS BELIEVE IT IS IMPORTANT FOR ORGANIZATIONS TO HAVE CYBERSECURITY-CERTIFIED EMPLOYEES.[12**]
Cyberattacks are growing, but the talent pool of defenders is not keeping pace.
Although attacks are growing in frequency and sophistication, the availability of sufficiently skilled cybersecurity professionals is falling behind. Cybersecurity Nexus (CSX) is addressing this gap by creating a skilled global cybersecurity workforce. From the Cybersecurity Fundamentals Certificate for university students to CSXP, the first vendor-neutral, performance-based cybersecurity certification, CSX is attracting and enabling cybersecurity professionals at every stage of their careers.
SOURCES: 1. 2015 Cost of Data Breach Study: Global Analysis, IBM and Ponemon Institute, May 2015. 2. ISACA 2015 APT Study, October 2015. 3. ISACA 2015 APT Study. 4. The Future of Cybercrime & Security: Financial and Corporate Threats & Mitigation, Juniper Research, May 2015. 5. SACA 2015 IT Risk/Reward Barometer-Member Study, September 2015. 6. ISACA 2015 IT Risk/Reward Barometer-Member Study. 7. UK House of Lords Digital Skills Committee. 8. Burning Glass Job Market Intelligence: Cybersecurity Jobs, 2015. 9. State of Cybersecurity: Implications for 2015, ISACA and RSA Conference, April 2015. 10. State of Cybersecurity: Implications for 2015. 11. Securing Our Future: Closing the Cyber Talent Gap, Raytheon and NCSA, October 2015. 12. 2015 ISACA Risk/Reward Barometer-Consumer Study, September 2015.
** "Employees" refers to data security professionals at organizations that potentially have access to survey respondent's personal information.
CSX CYBERSECURITY NEXUS
ISACA Trust in, and value from, information systems
https://cybersecurity.isaca.org
January 2016

The Phases of Ethical Hacking

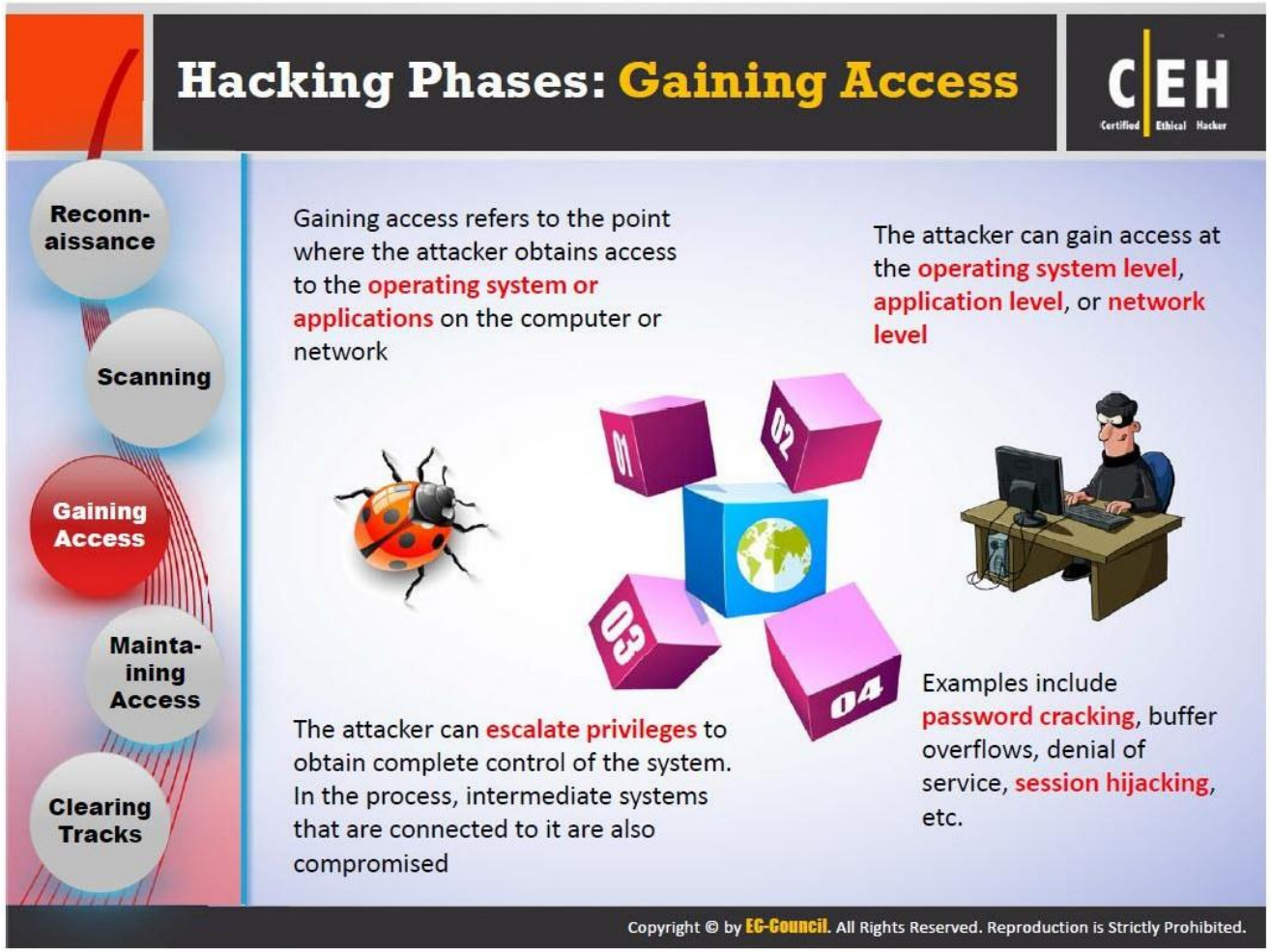
Reconnaissance



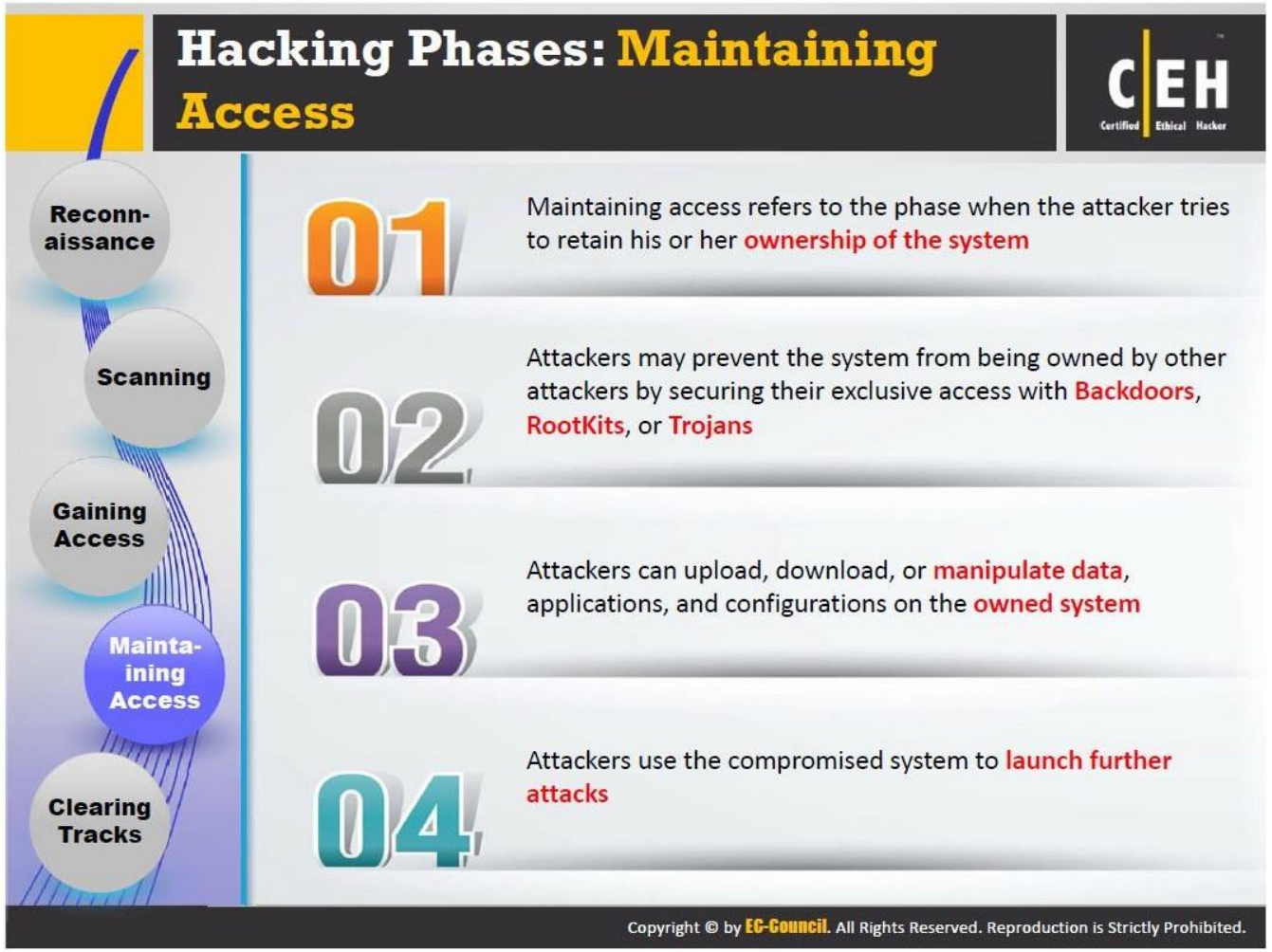
Scanning


Hacking Phases: Scanning
C|EH
Certified Ethical Hacker
Recon-aissance
Scanning
Gaining Access
Mainta-ining Access
Clearing Tracks
Pre-Attack Phase
Scanning refers to the pre-attack phase when the attacker scans the network for specific information on the basis of information gathered during reconnaissance
Scanning can include use of dialers, port scanners, network mappers, ping tools, vulnerability scanners, etc.
Port Scanner
Extract Information
Attackers extract information such as live machines, port, port status, OS details, device type, system uptime, etc. to launch attack
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

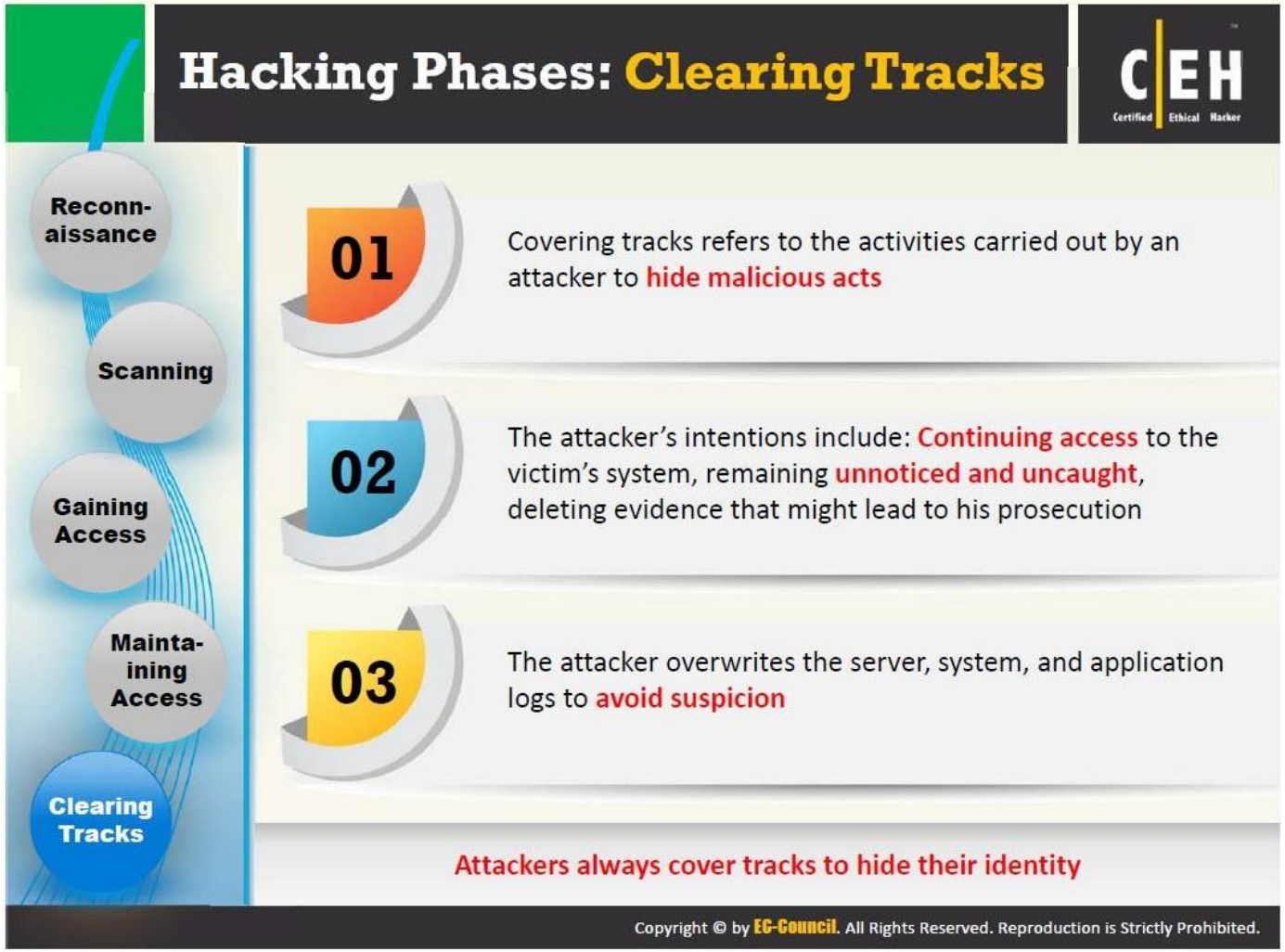
Gaining Access



Maintaining Access



Clearing Tracks



Network vs Web Browser Attacks

Objectives of Footprinting

Objectives of Footprinting

C|EH Certified Ethical Hacker

Collect Network Information

- Domain name
- Internal domain names
- Network blocks
- IP addresses of the reachable systems
- Rogue websites/private websites
- TCP and UDP services running
- Access control mechanisms and ACL's
- Networking protocols
- VPN Points
- IDSes running
- Analog/digital telephone numbers
- Authentication mechanisms
- System enumeration

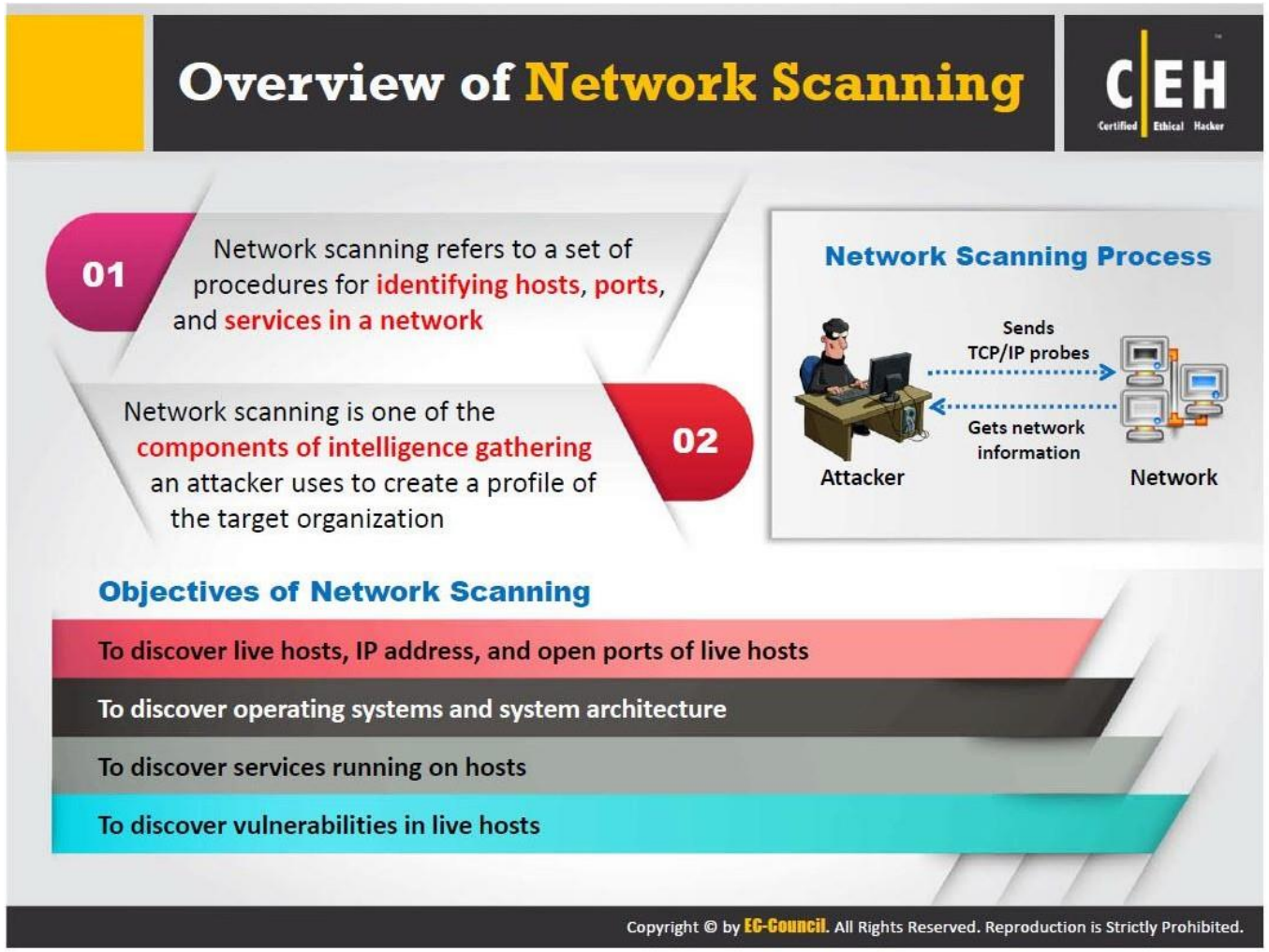
Collect System Information

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

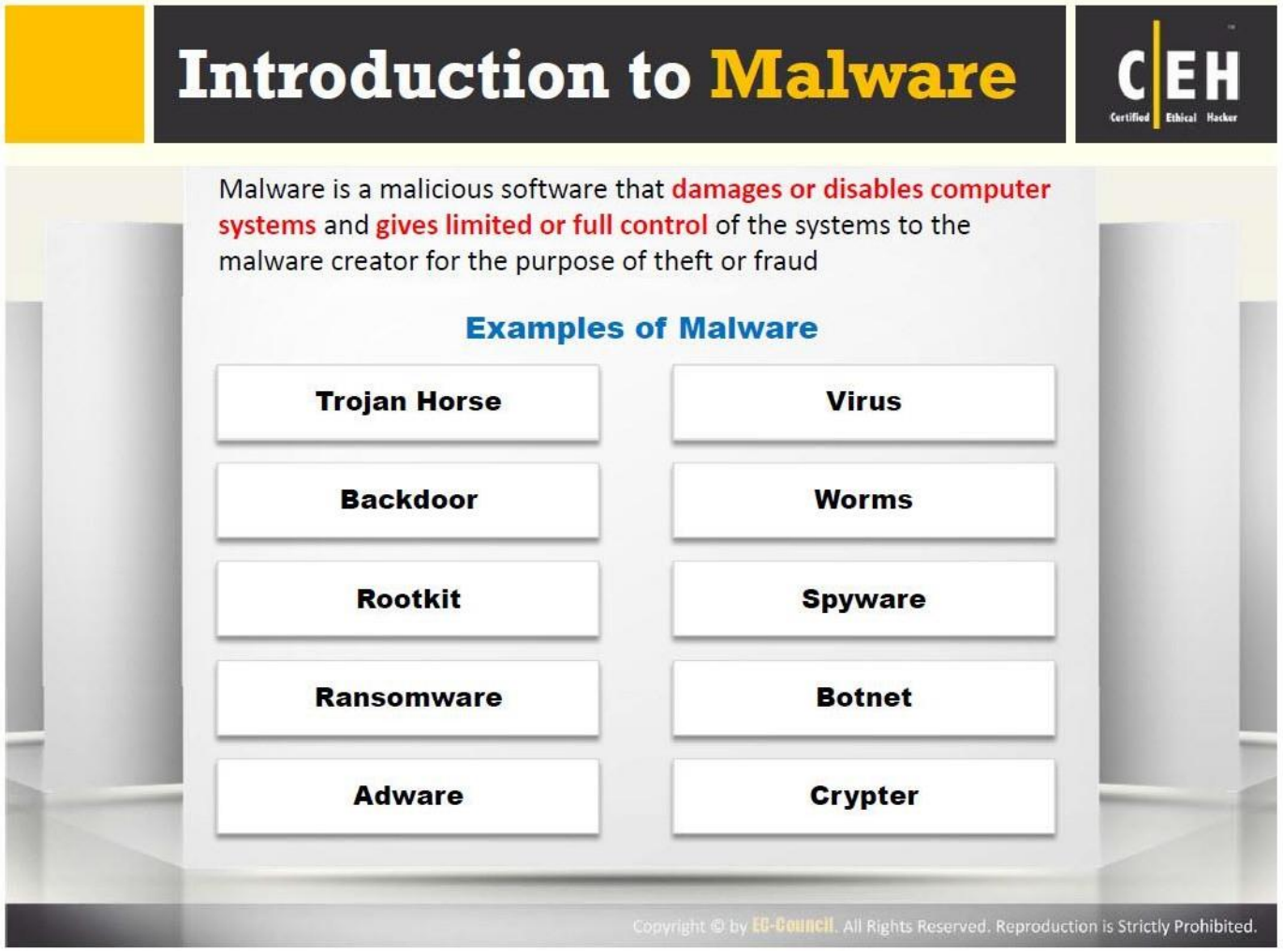
Collect Organization's Information

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

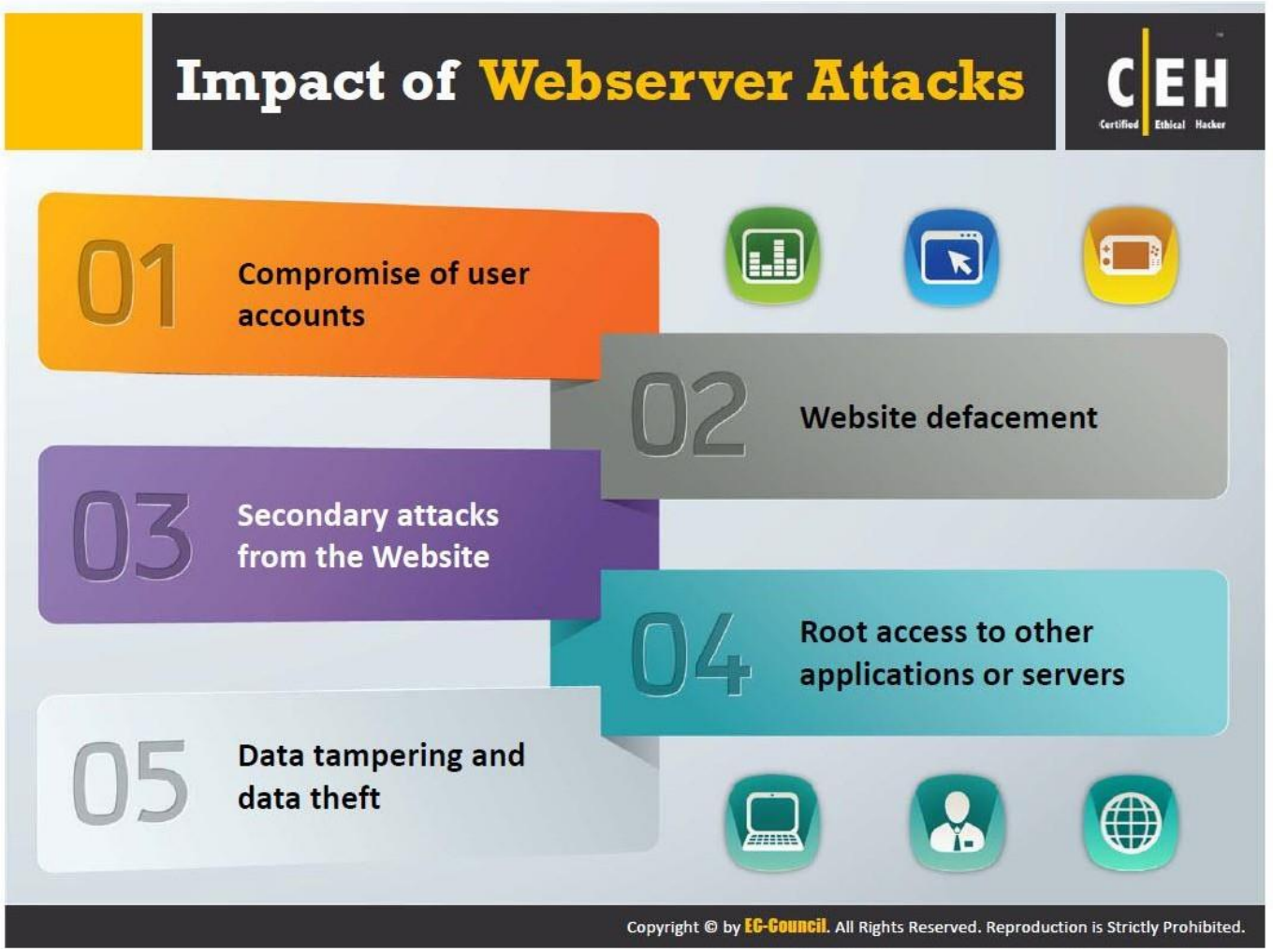
Overview of Network Scanning



Introduction to Malware



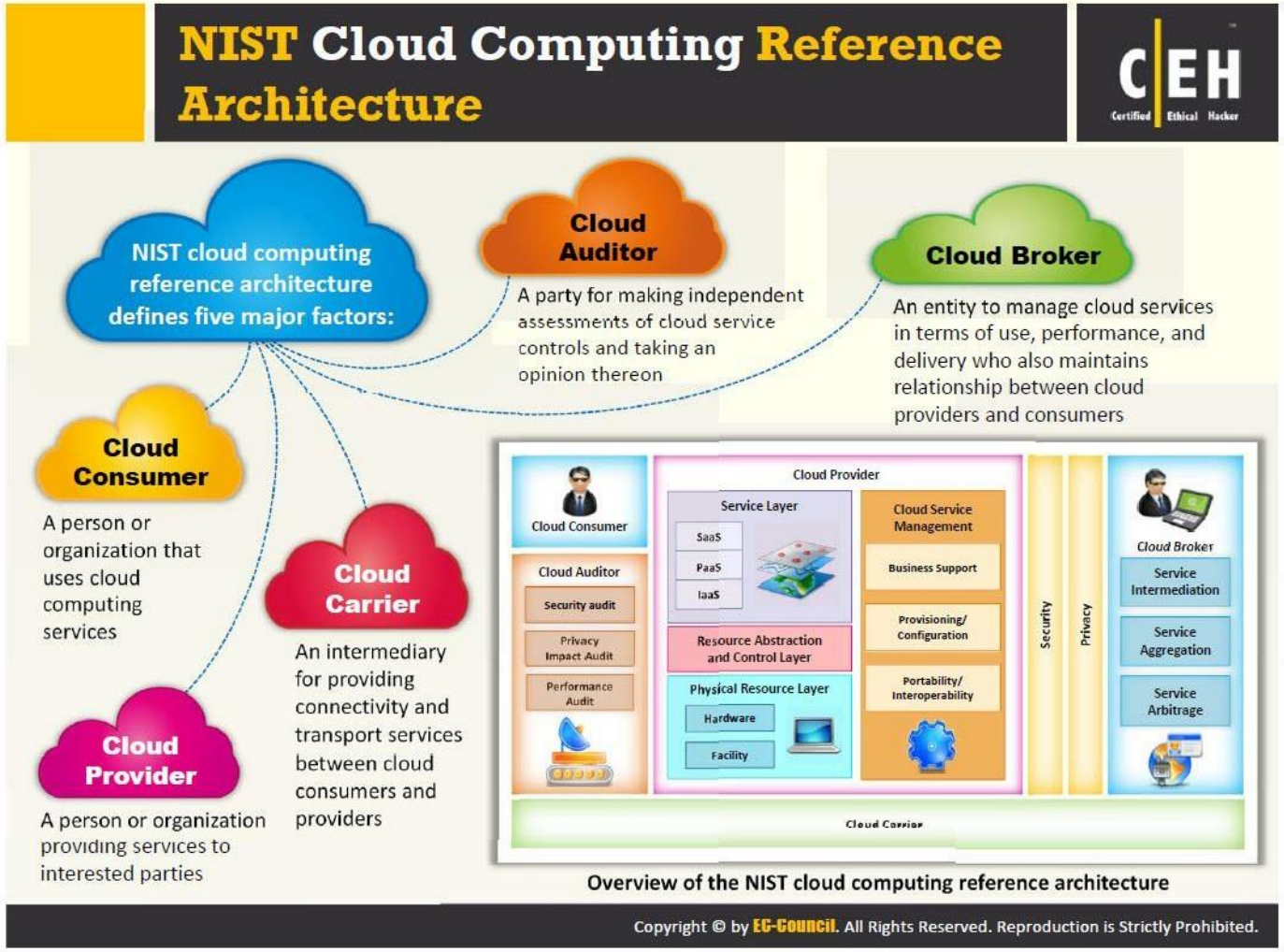
Impact of Webserver Attacks



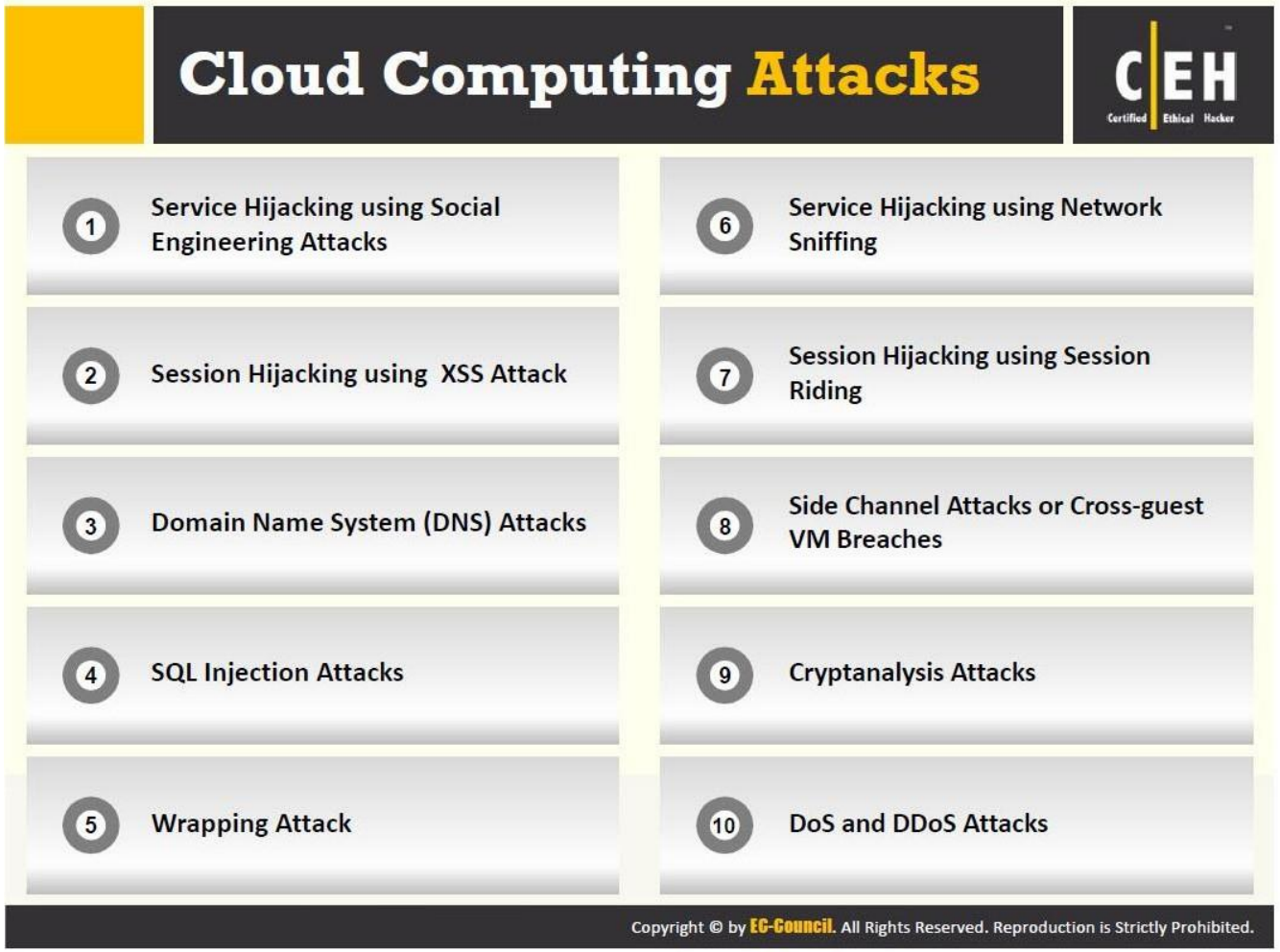
Web Application Attacks

Who is Responsible for my Data in the Cloud

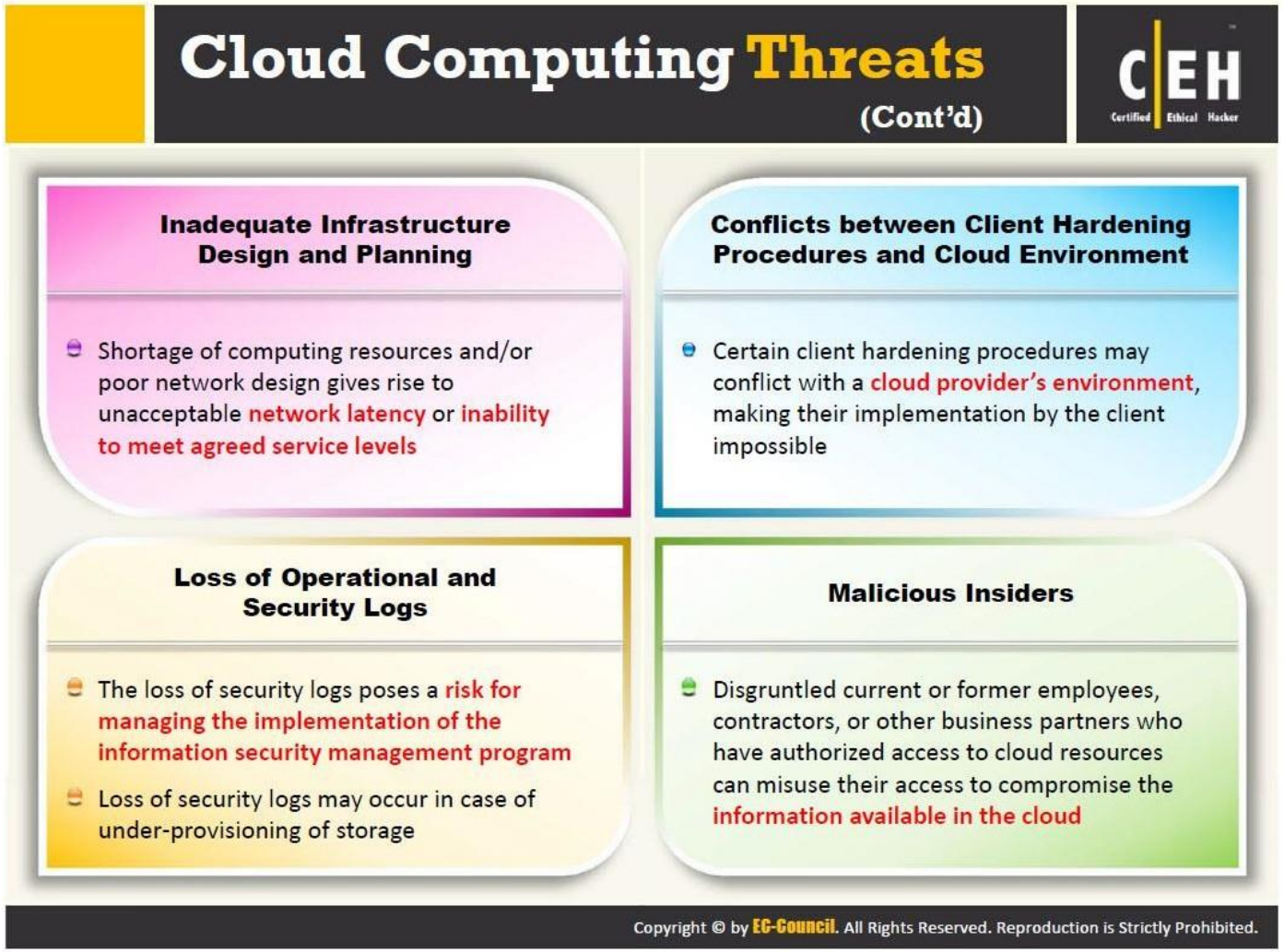
NIST Cloud Computing Reference Architecture



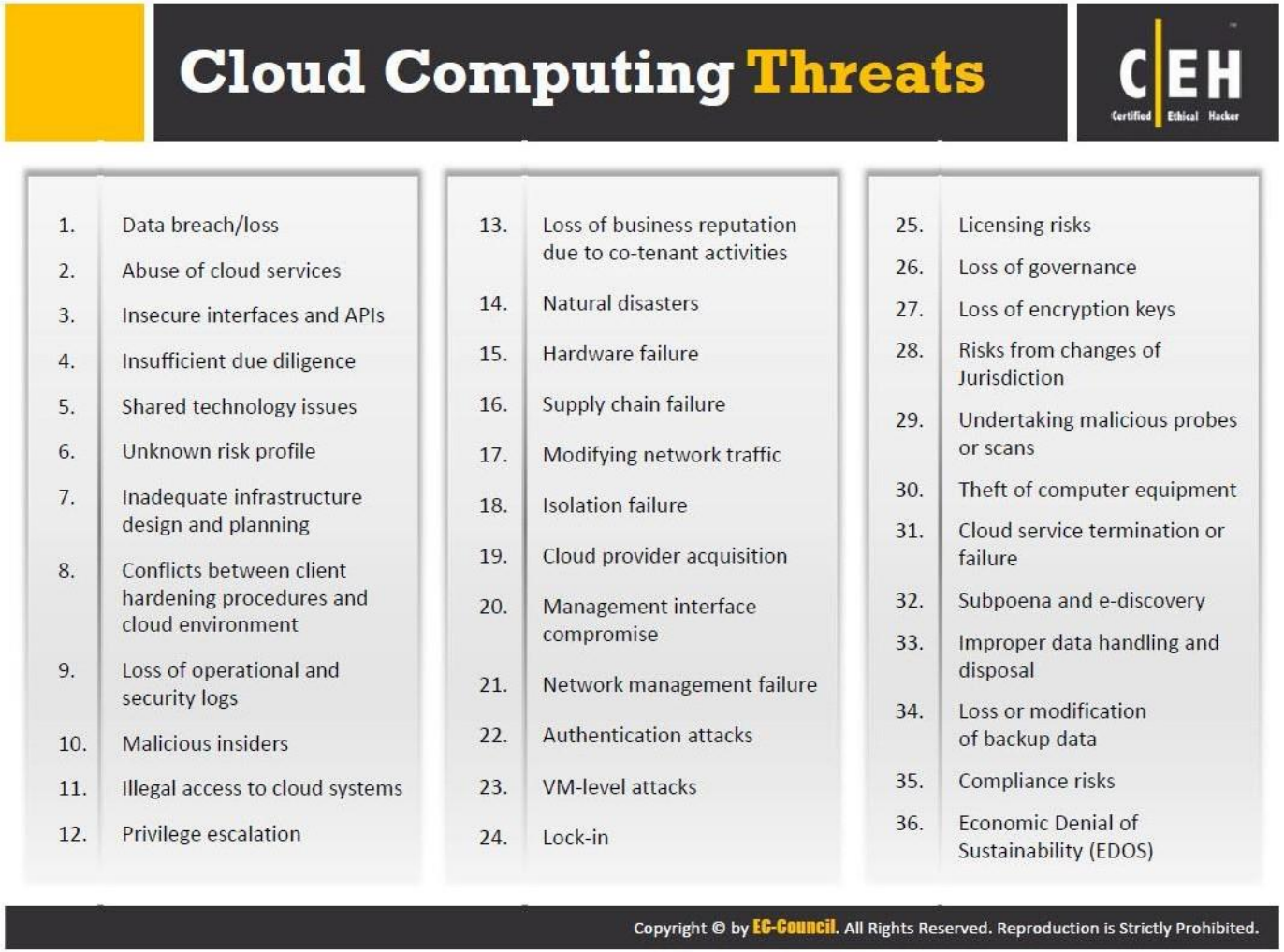
Cloud Computing Attacks



Cloud Computing Threats

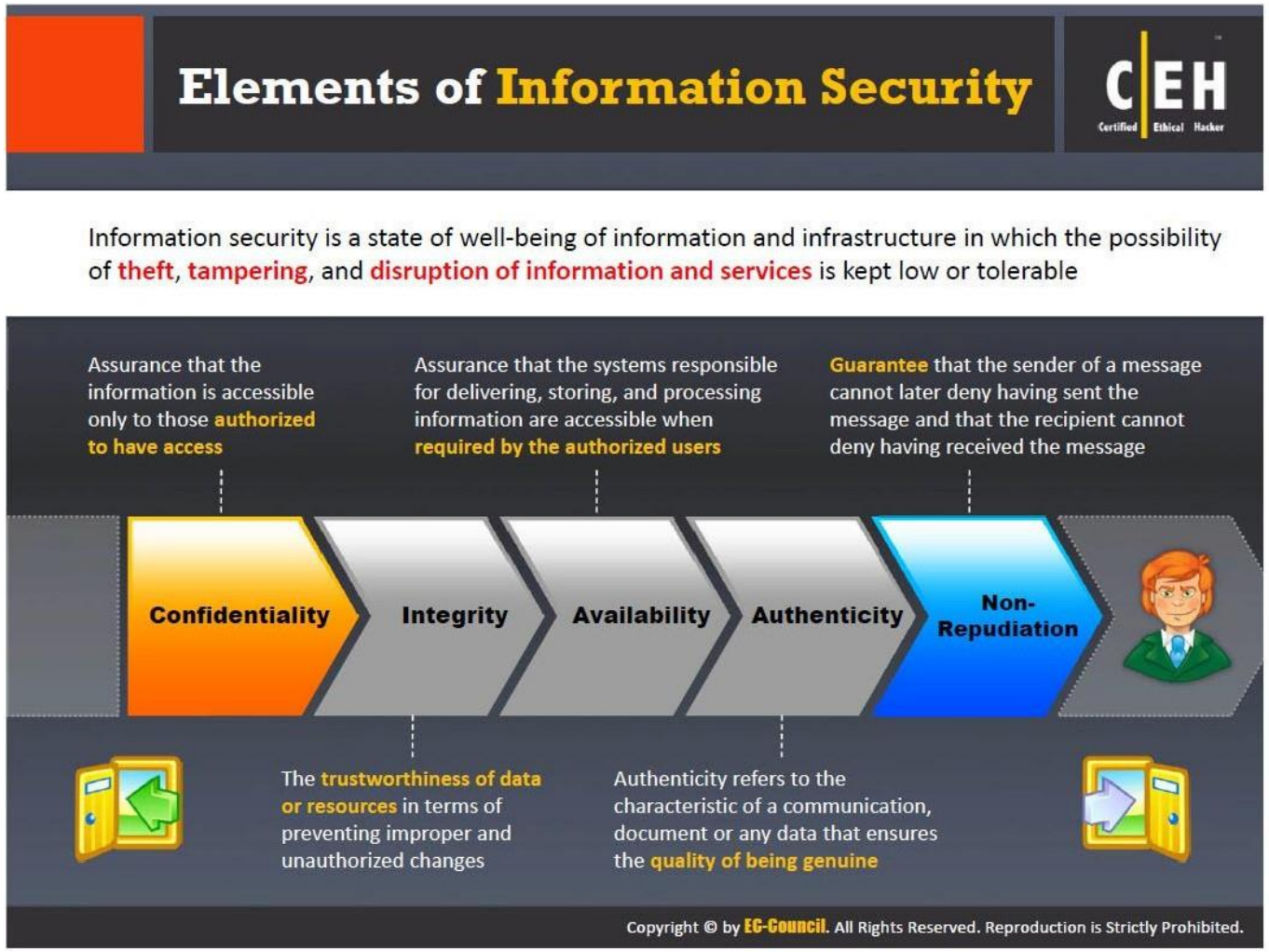


Cloud Computing Threats

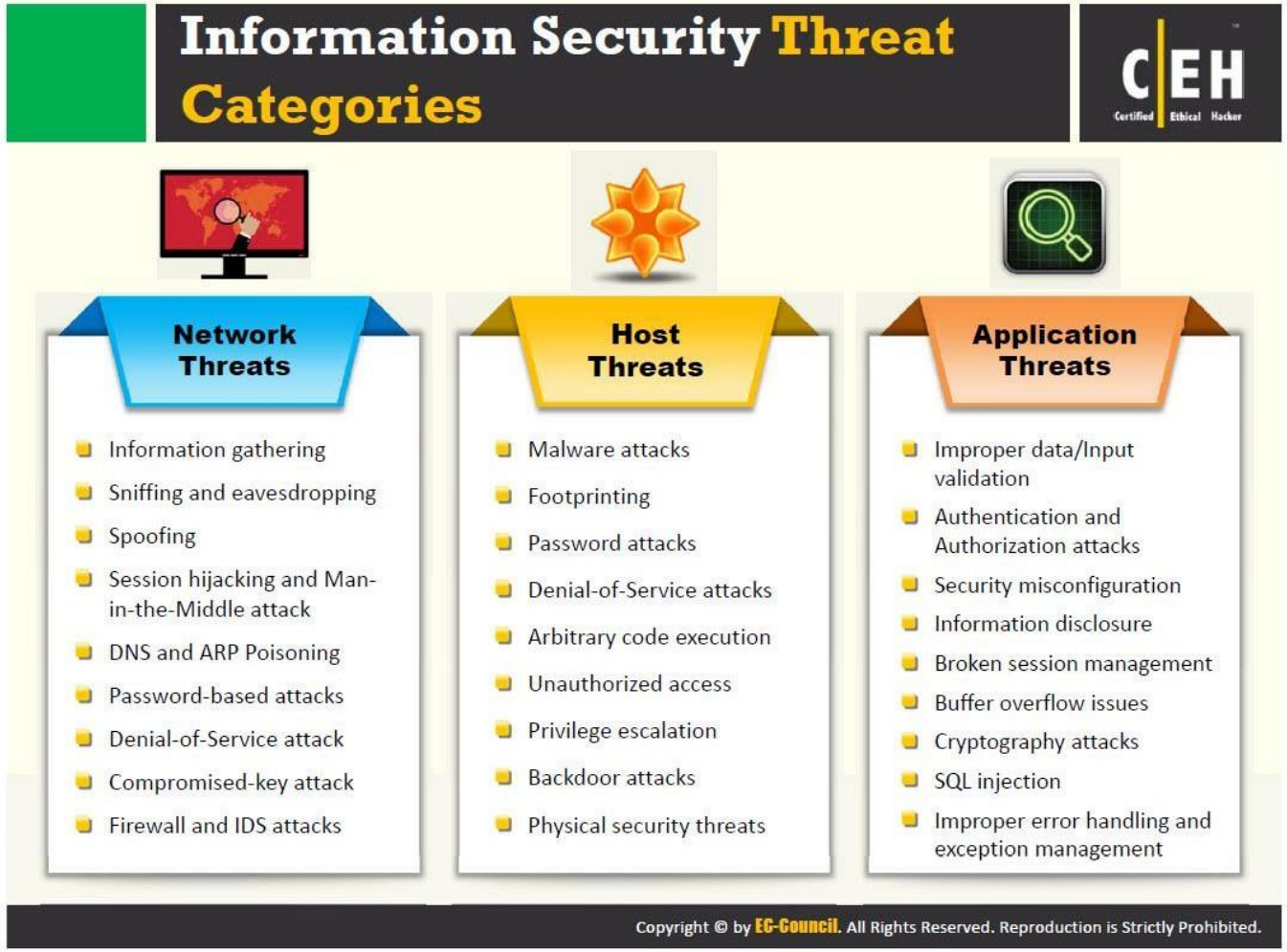


Vulnerability Assessments & Penetration Testing

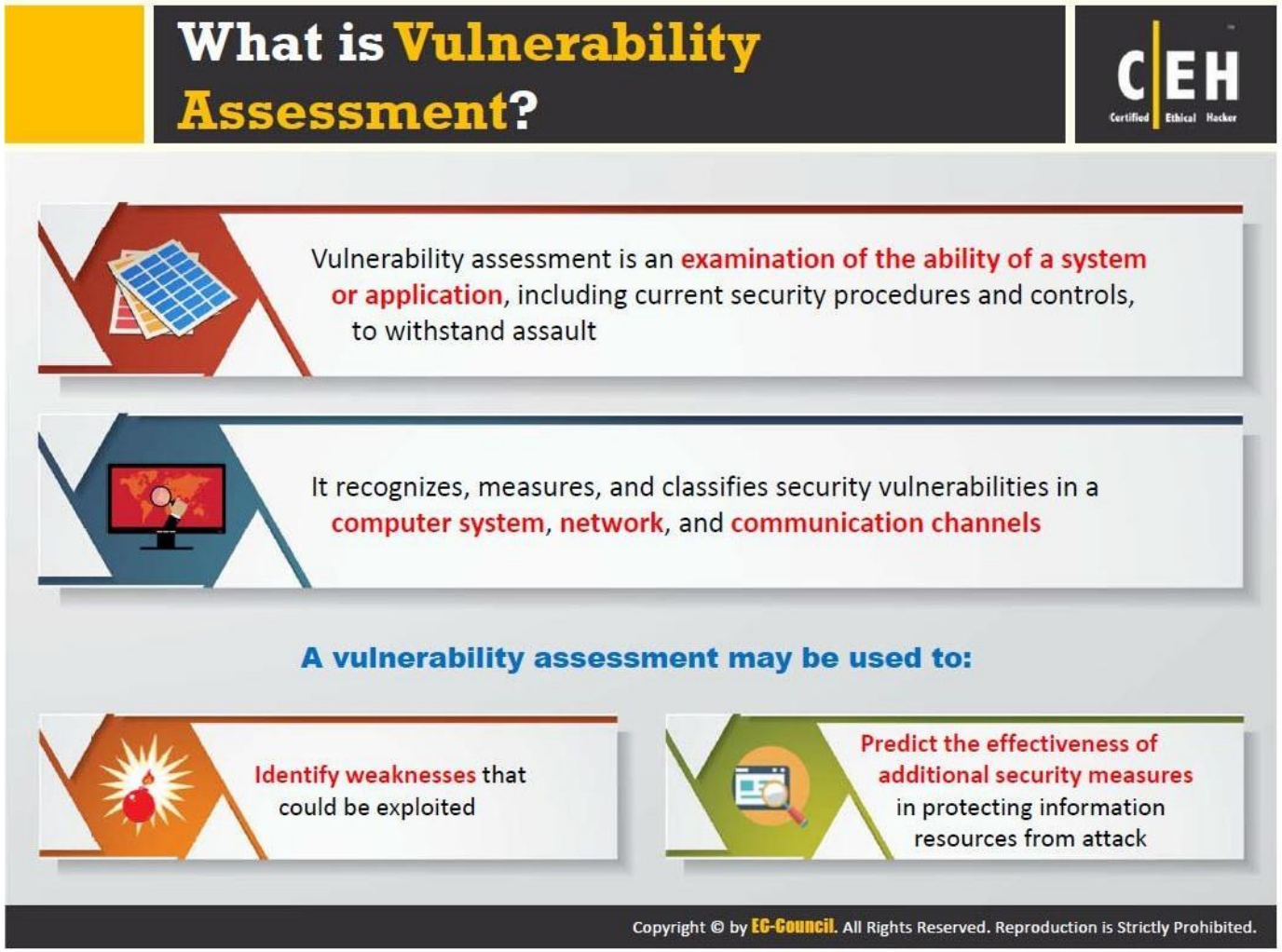
Elements of Information Security



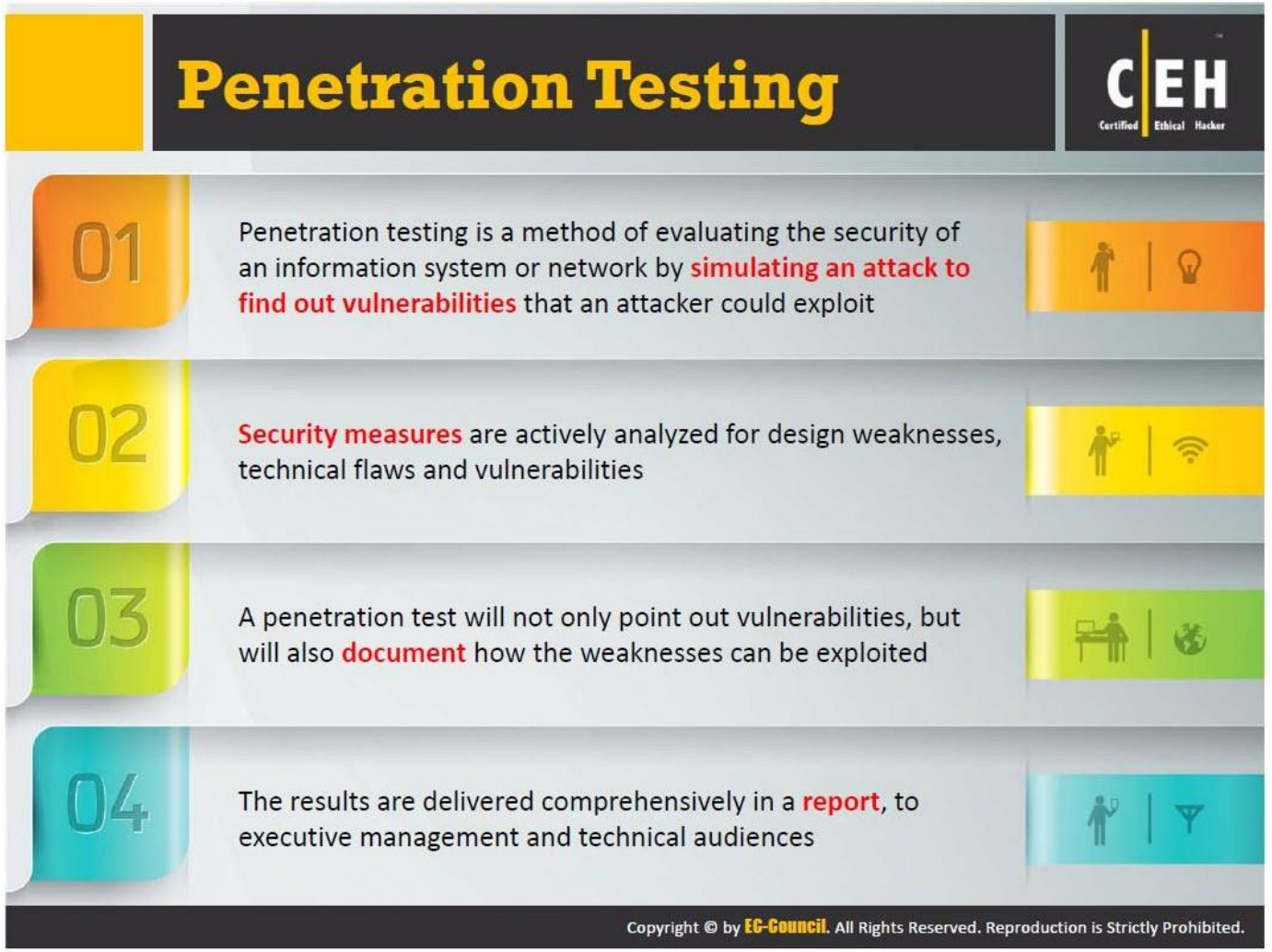
Information Security Threat Categories



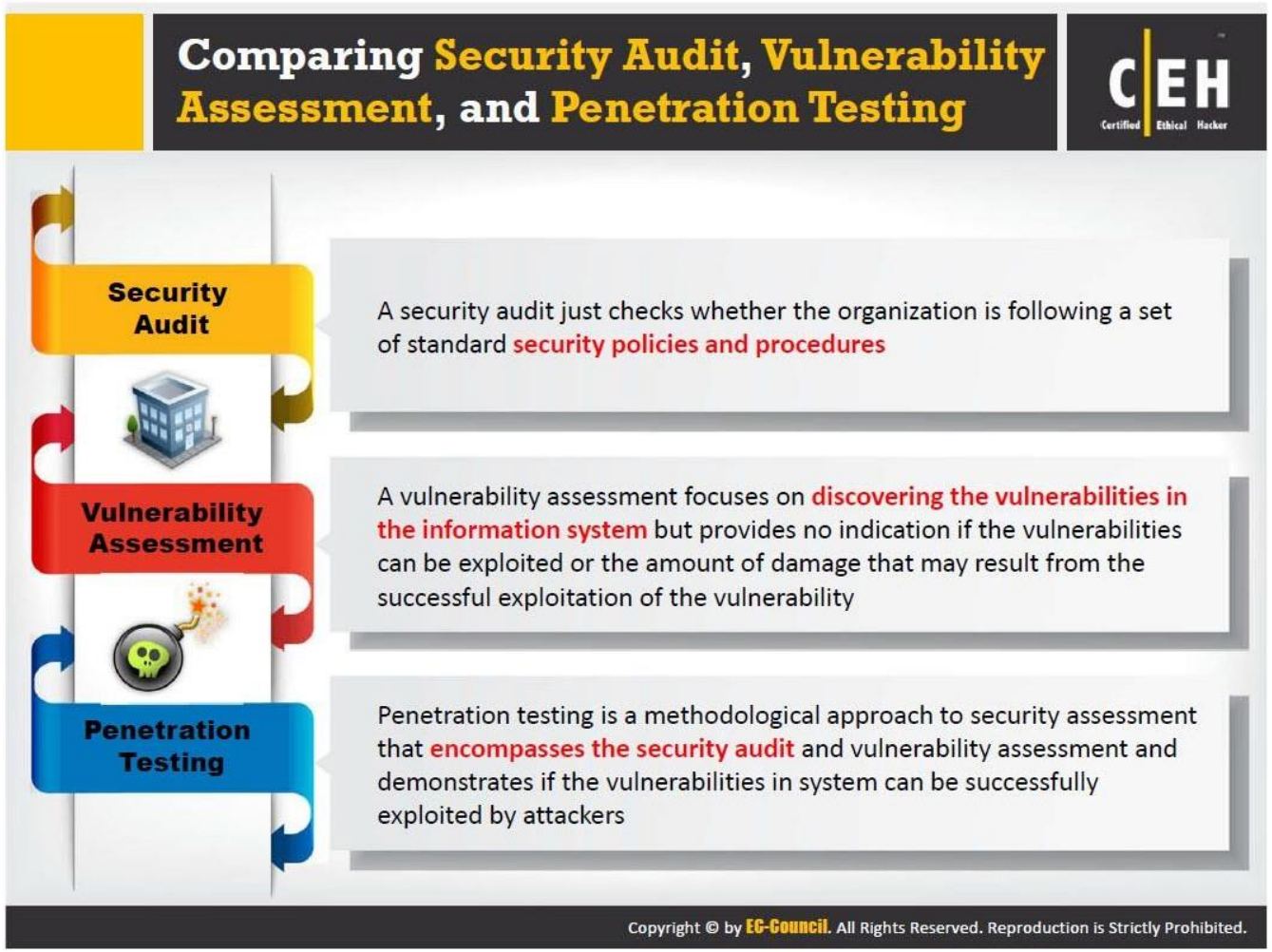
What is Vulnerability Assessment?



Penetration Testing

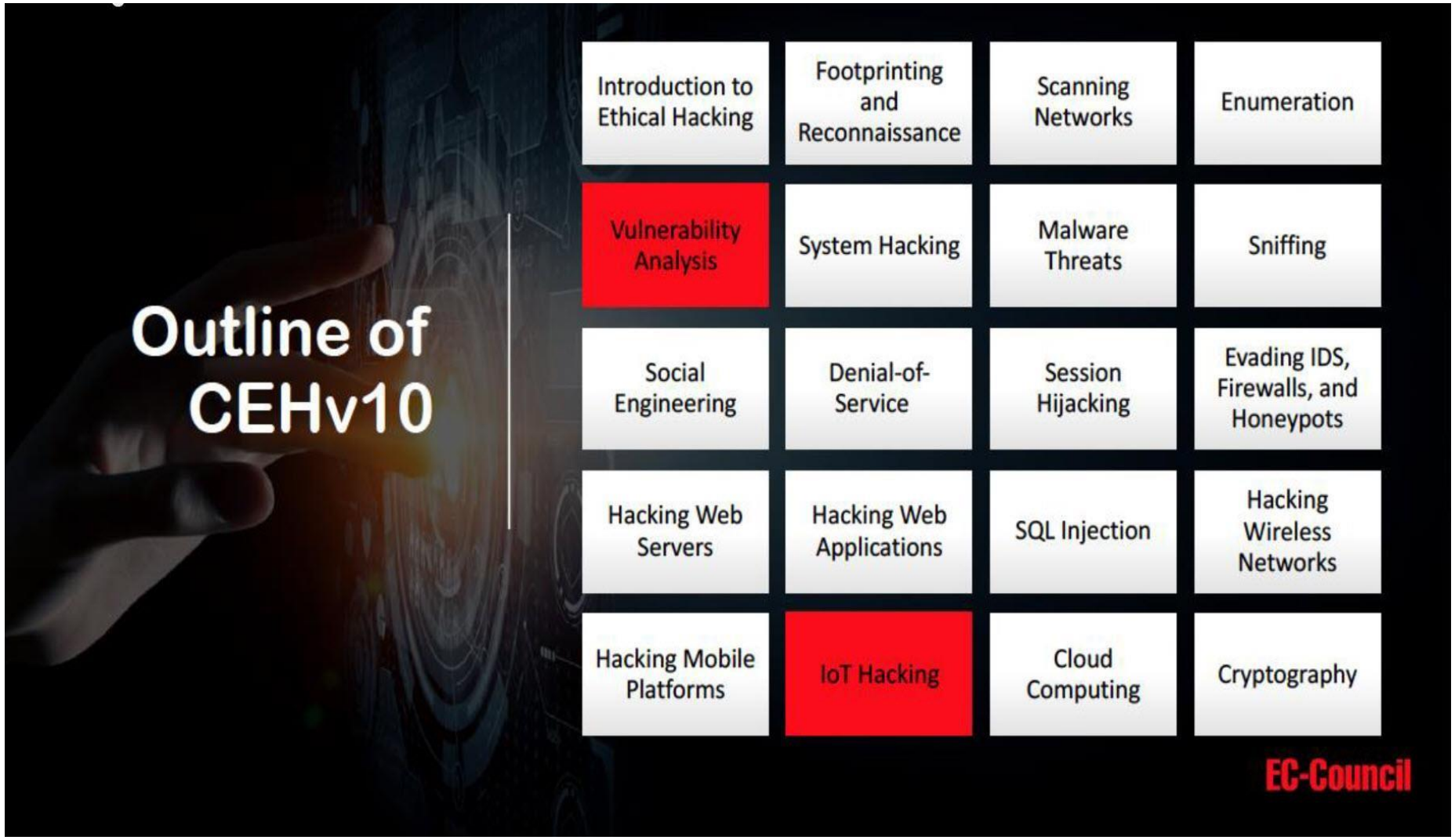


Security Audit vs Vulnerability Assessment vs Penetration Testing

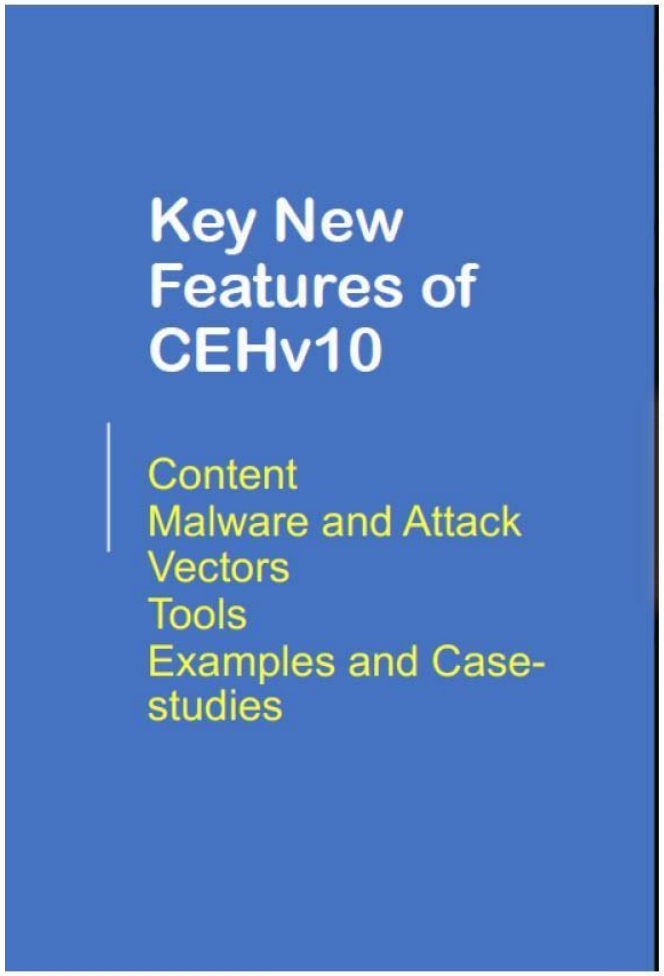


What is in the Course

Outline


Outline of CEHv10
Introduction to Ethical Hacking
Footprinting and Reconnaissance
Scanning Networks
Enumeration
Vulnerability Analysis
System Hacking
Malware Threats
Sniffing
Social Engineering
Denial-of-Service
Session Hijacking
Evading IDS, Firewalls, and Honeypots
Hacking Web Servers
Hacking Web Applications
SQL Injection
Hacking Wireless Networks
Hacking Mobile Platforms
IoT Hacking
Cloud Computing
Cryptography
EC-Council

New Features



Inclusion New Modules – Vulnerability Analysis

Inclusion of complete Malware Analysis Process

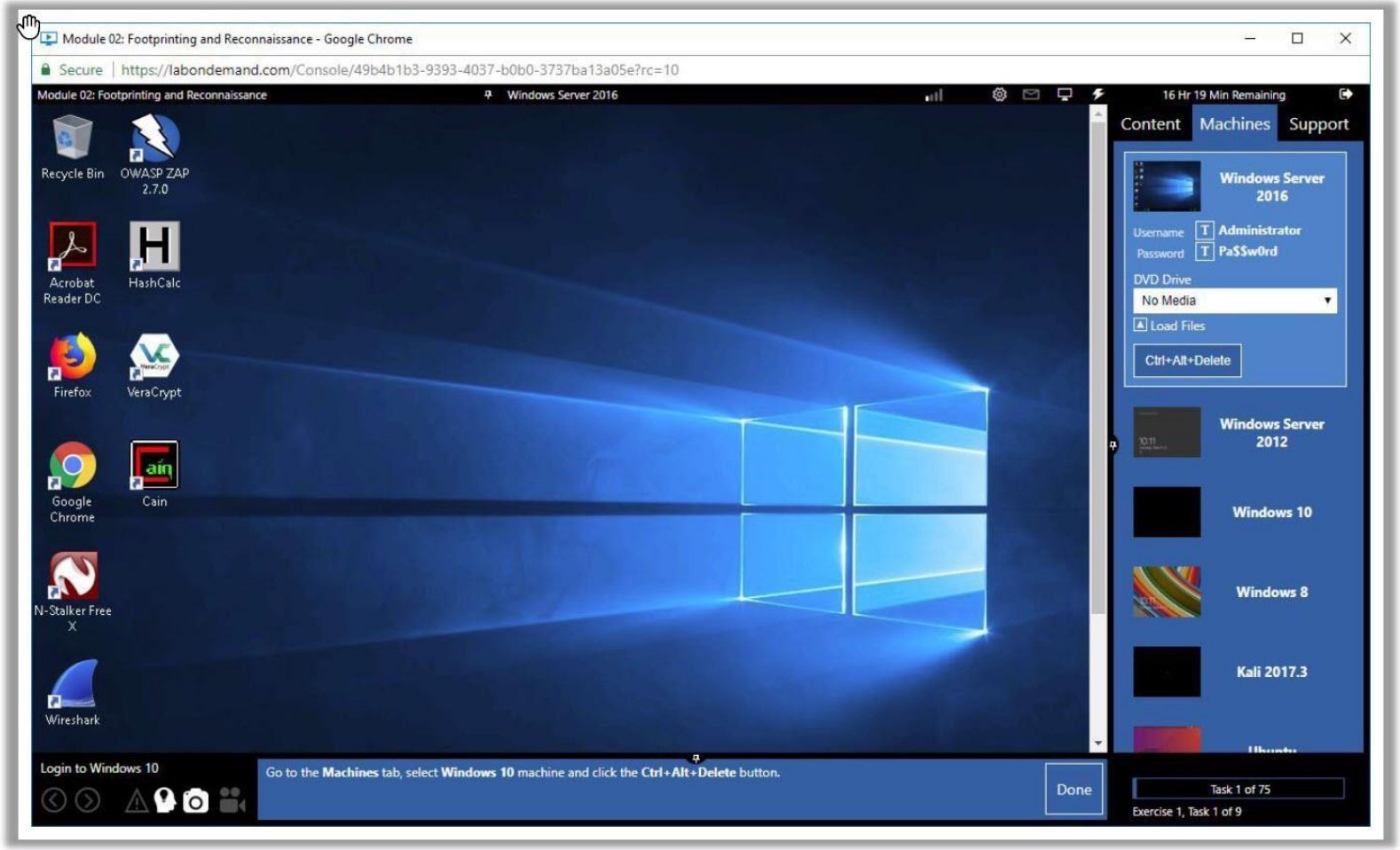
Inclusion New Modules – IoT Hacking

Latest hacking tools (Based on Windows, MAC, Linux, and Mobile)

100% Compliance to NICE 2.0 Framework

Focus on Emerging Attack Vectors - Cloud, AI, ML, etc.

Windows Server 2016 Machine in iLabs



Practical

nstructor Guide

CEH Practical Credential

- CEH Practical EXAM is a 6 hours practical exam
- 20 real-life scenarios that requires them to demonstrate the application of ethical hacking techniques
- Remote online proctored

CEH Practical Credential

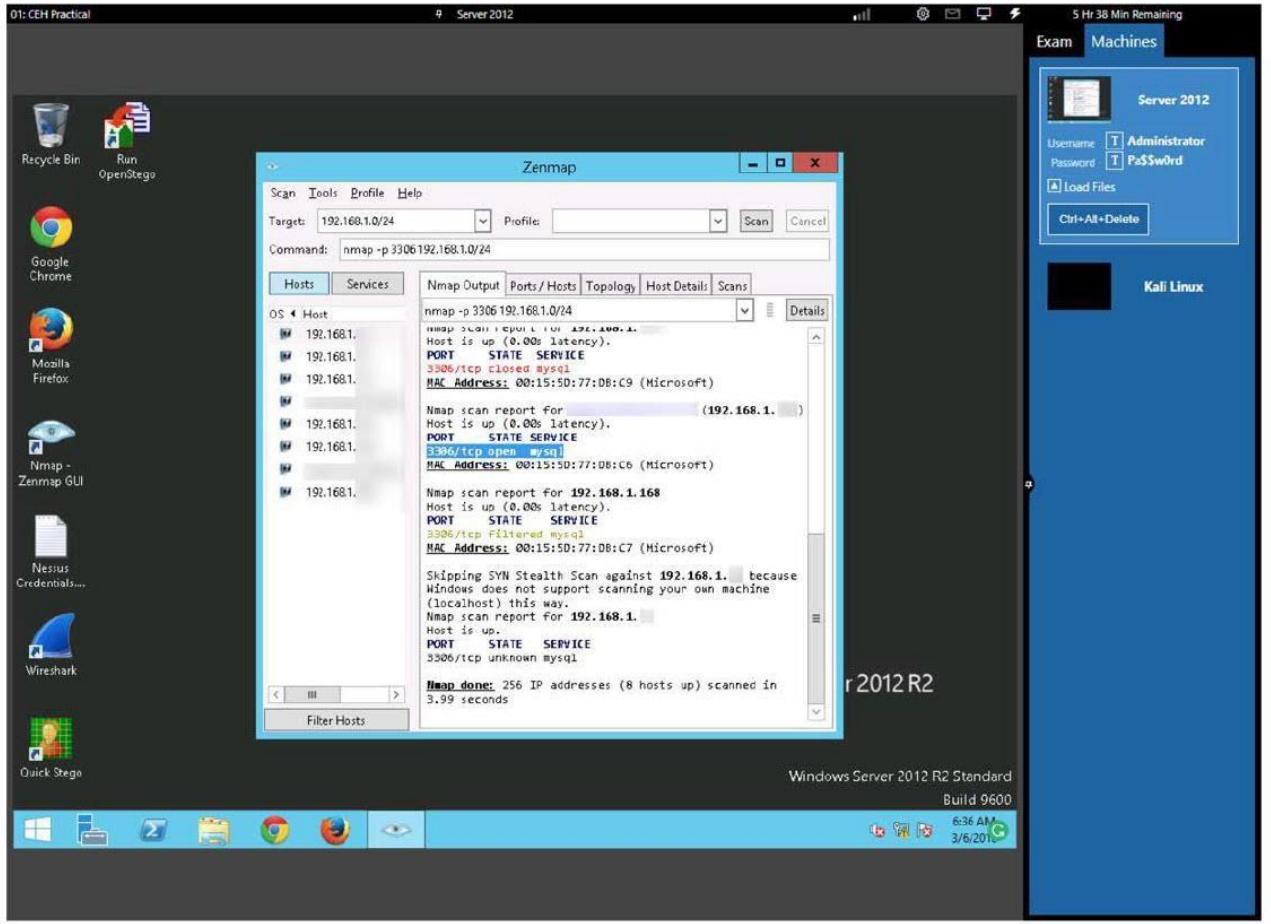
Q: During a security assessment, it was found that a server was hosting a website that was vulnerable to certain types of web attacks. Further investigation revealed that the underlying database management system of the site was MySQL. Determine the OS of the machine which hosted the database.

a. Windows Server 2012

b. Windows 8.1

c. Ubuntu

d. Windows Server 2008



THANK YOU !!!