

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

Shirey

Informational

[Page 1]

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?

What is Hacking?



Hacking refers to exploiting **system vulnerabilities** and **compromising security** controls to gain unauthorized or inappropriate access to the system resources



It involves **modifying system or application features** to achieve a goal outside of the creator's original purpose



Hacking can be used to steal, pilfer, and redistribute intellectual property leading to **business loss**

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

Who is a Hacker?

Who is a Hacker?

C|EH
Certified Ethical Hacker

- 01**
Intelligent individuals with excellent computer skills, with the ability to create and explore into the computer's software and hardware
- 02**
For some hackers, hacking is a hobby to see how many computers or networks they can compromise
- 03**
Their intention can either be to gain knowledge or to poke around to do illegal things

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

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

What is Ethical Hacking?

The infographic is titled "What is Ethical Hacking?" in large white and yellow text. It features the CEH logo (Certified Ethical Hacker) in the top right corner. The content is organized into three main sections, each with an icon and text:

- Ethical hacking involves the use of hacking tools, tricks, and techniques to identify vulnerabilities so as to ensure system security.** (Icon: Laptop with network connections)
- It focuses on simulating techniques used by attackers to verify the existence of exploitable vulnerabilities in the system security.** (Icon: Laptop with a magnifying glass over a code editor)
- Ethical hackers performs security assessment of their organization with the permission of concerned authorities** (Icon: Computer monitor displaying user icons)

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

Why Ethical Hacking is Necessary?

Why Ethical Hacking is Necessary

CEH
Certified Ethical Hacker

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

Ethical hacking is necessary as it **allows to counter attacks from malicious hackers** by anticipating methods used by them to break into a system

Reasons why Organizations Recruit Ethical Hackers



- To prevent **hackers** from gaining access to organization's information systems
- To uncover **vulnerabilities** in systems and explore their potential as a risk
- To analyze and **strengthen an organization's security posture** including policies, network protection infrastructure, and end-user practices

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

Why Ethical Hacking is Necessary?

Why Ethical Hacking is Necessary

(Cont'd)



Ethical Hackers Try to Answer the Following Questions



What can the intruder see on the **target system**? (Reconnaissance and Scanning phases)



What can an **intruder do** with that information? (Gaining Access and Maintaining Access phases)



Does anyone at the target **notice the intruders' attempts** or successes?
(Reconnaissance and Covering Tracks phases)



If all the **components of information system** are adequately protected, updated, and patched



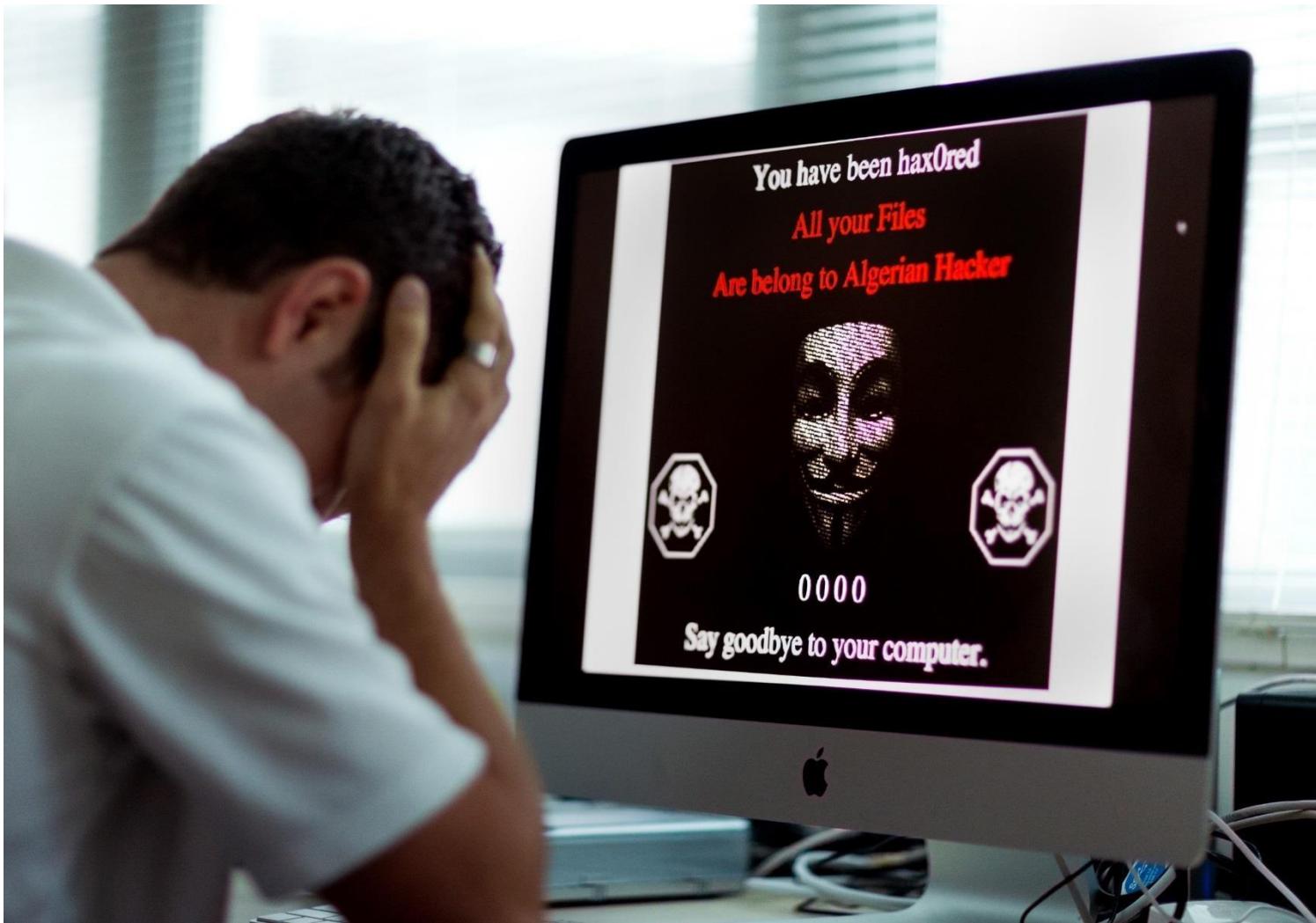
How much effort, time, and money is required to obtain **adequate protection**?



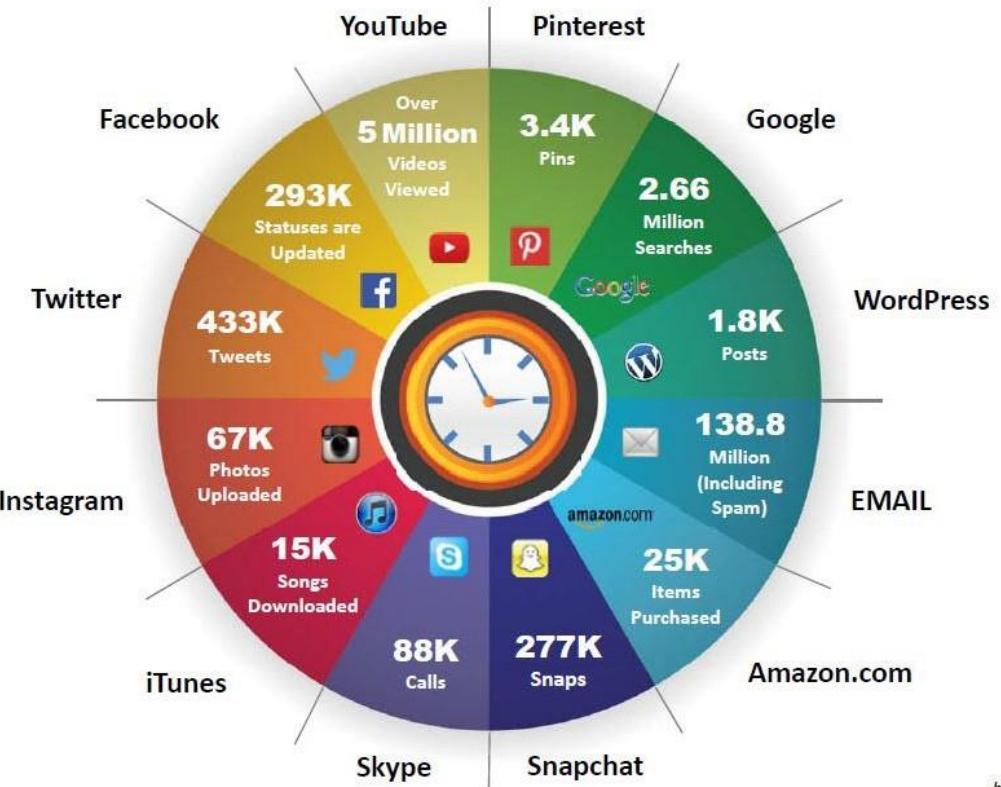
Are the **information security measures** in compliance to industry and legal standards?

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

Why Should I Care

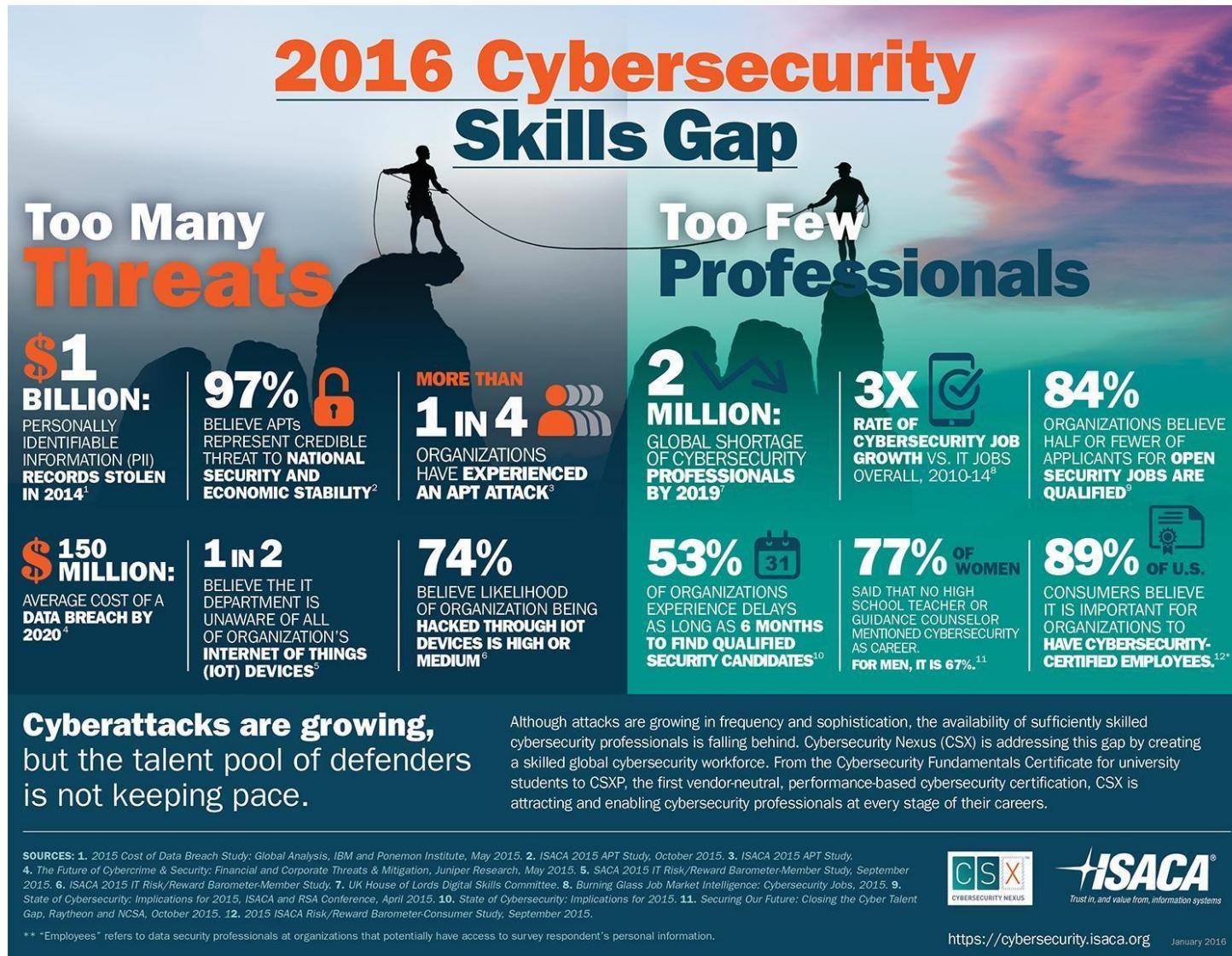


Internet is Integral Part of Business and Personal Life - What Happens Online in 60 Seconds



<http://blog.qmee.com>

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



The Phases of Ethical Hacking

Hacking Phases: Reconnaissance

CEH
Certified Ethical Hacker

The diagram illustrates the five phases of hacking as a vertical sequence of five circles. From top to bottom, the phases are: **Reconnaisance** (green), **Scanning** (grey), **Gaining Access** (grey), **Maintaining Access** (grey), and **Clearing Tracks** (grey). The background features a light blue gradient with radiating lines.

Reconnaisance

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

Reconnaisance Types

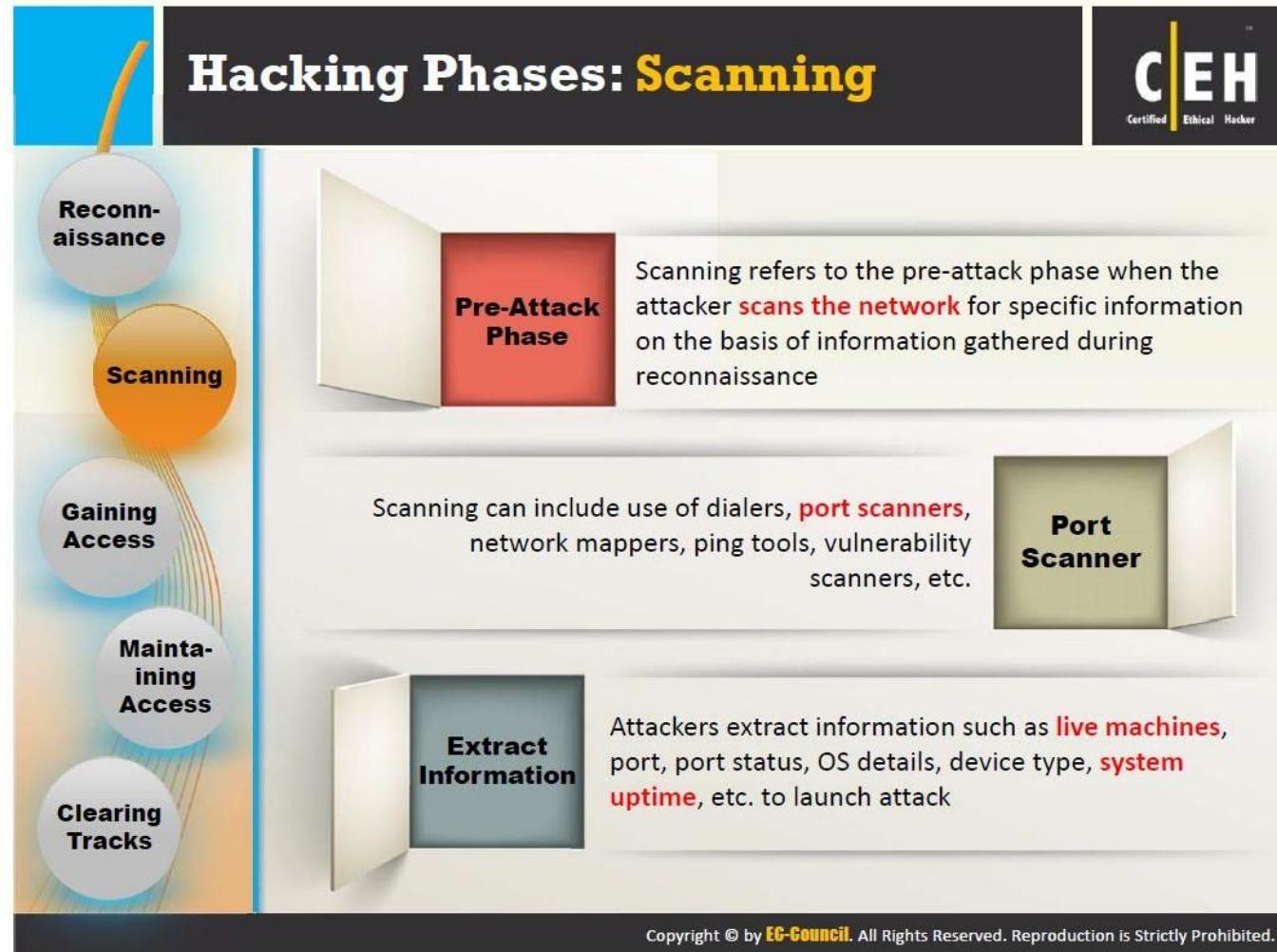
Passive Reconnaissance

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

Active Reconnaissance

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

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



Hacking Phases: Gaining Access

The Certified Ethical Hacker (CEH) logo is visible in the top right corner.



The diagram shows five circular phases stacked vertically on the left side:

- Reconnaisance
- Scanning
- Gaining Access (highlighted in red)
- Maintaining Access
- Clearing Tracks

Gaining access refers to the point where the attacker obtains access to the **operating system or applications** on the computer or network. The attacker can gain access at the **operating system level, application level, or network level**.

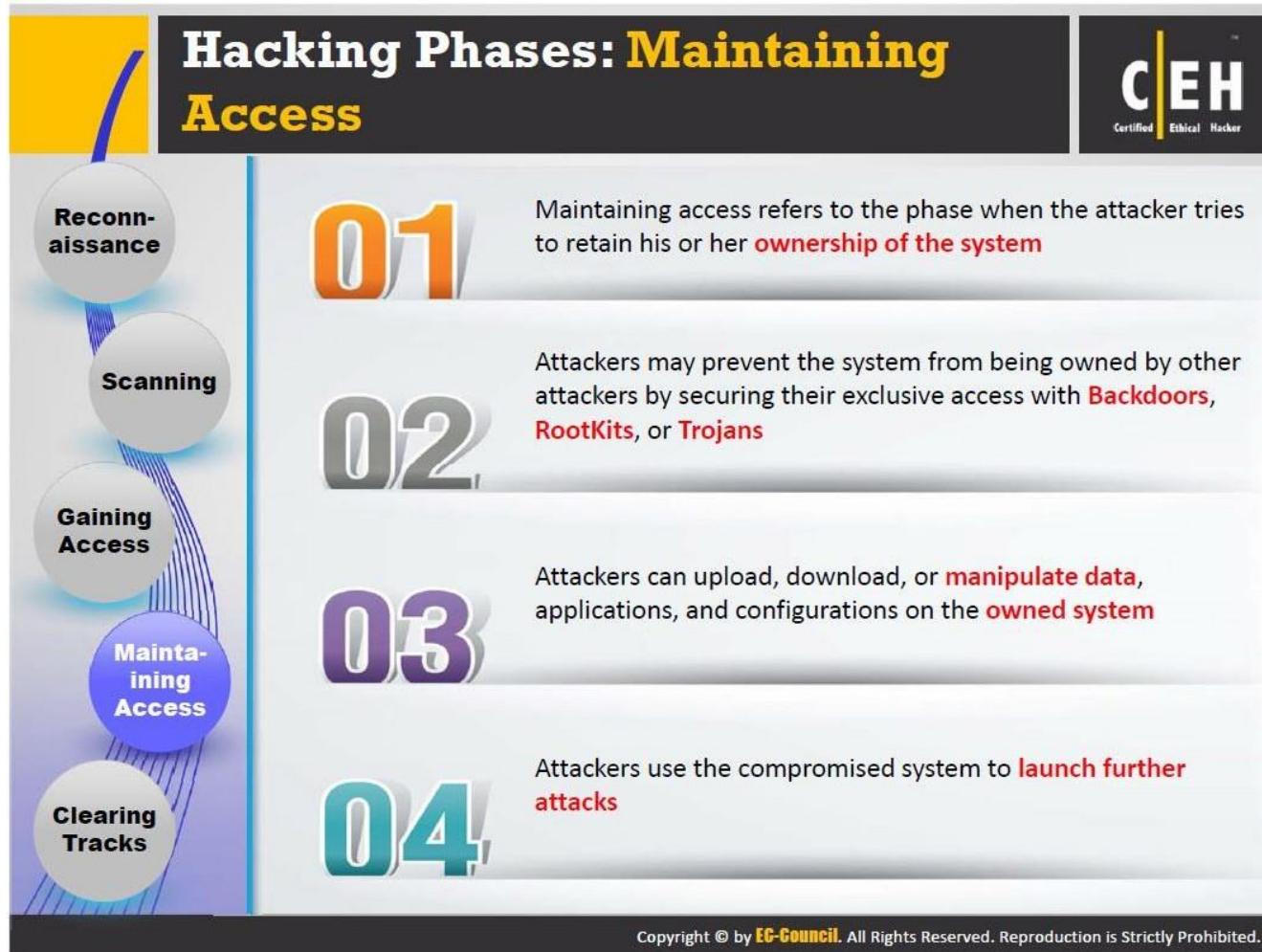
The attacker can **escalate privileges** to obtain complete control of the system. In the process, intermediate systems that are connected to it are also compromised.

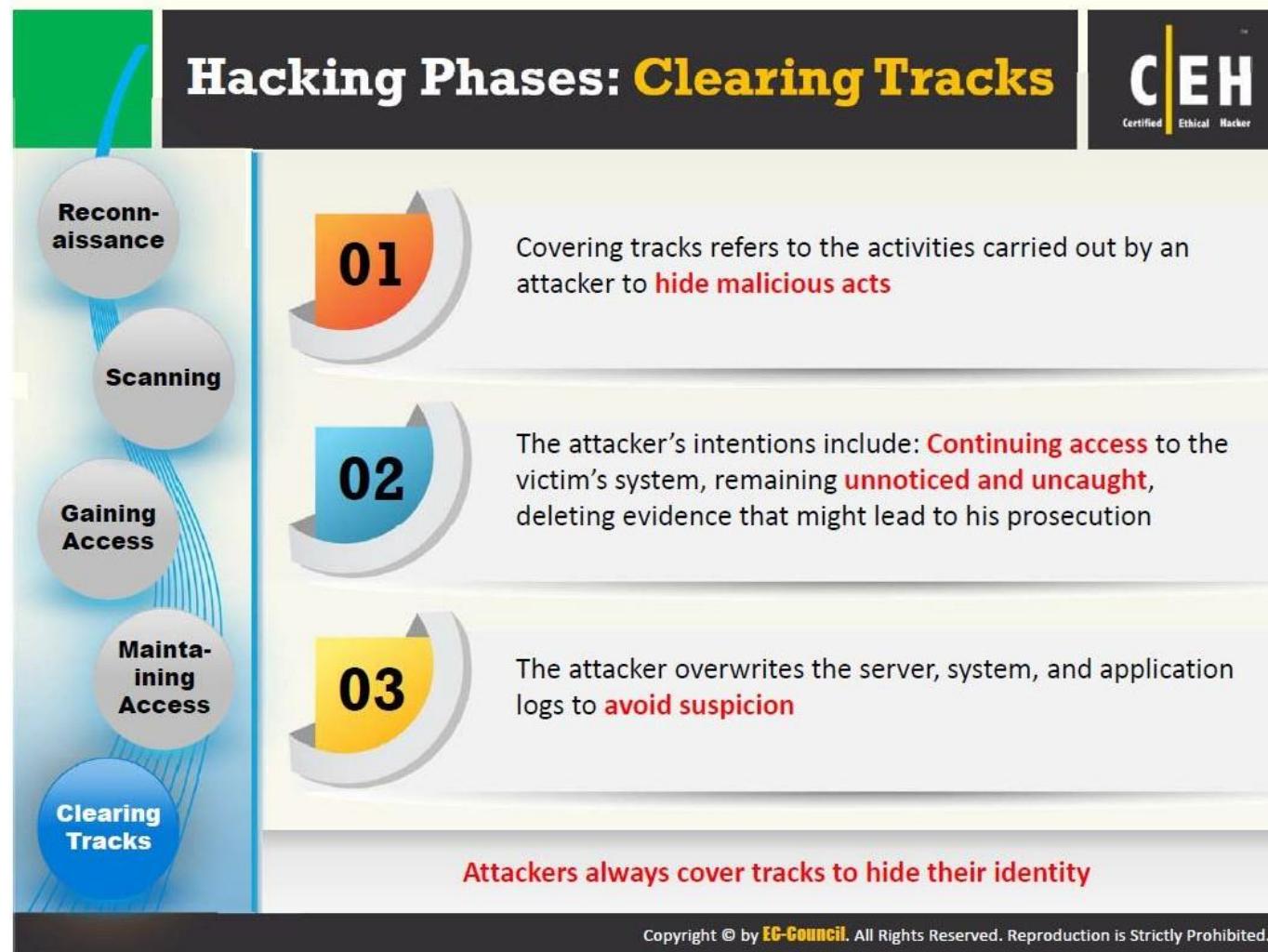


Examples include **password cracking, buffer overflows, denial of service, session hijacking, etc.**

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

Maintaining Access





Network vs Web Browser Attacks

Objectives of Footprinting

Objectives of Footprinting

CEH
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
- IDSe 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

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

Overview of Network Scanning

Overview of Network Scanning

CEH
Certified Ethical Hacker

01 Network scanning refers to a set of procedures for **identifying hosts, ports, and services in a network**

02 Network scanning is one of the **components of intelligence gathering** an attacker uses to create a profile of the target organization

Network Scanning Process

The diagram shows an "Attacker" at a computer sending "TCP/IP probes" to a "Network" of three computer icons. The network then "Gets network information" and returns it to the attacker.

Objectives of Network Scanning

- To discover live hosts, IP address, and open ports of live hosts
- To discover operating systems and system architecture
- To discover services running on hosts
- To discover vulnerabilities in live hosts

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

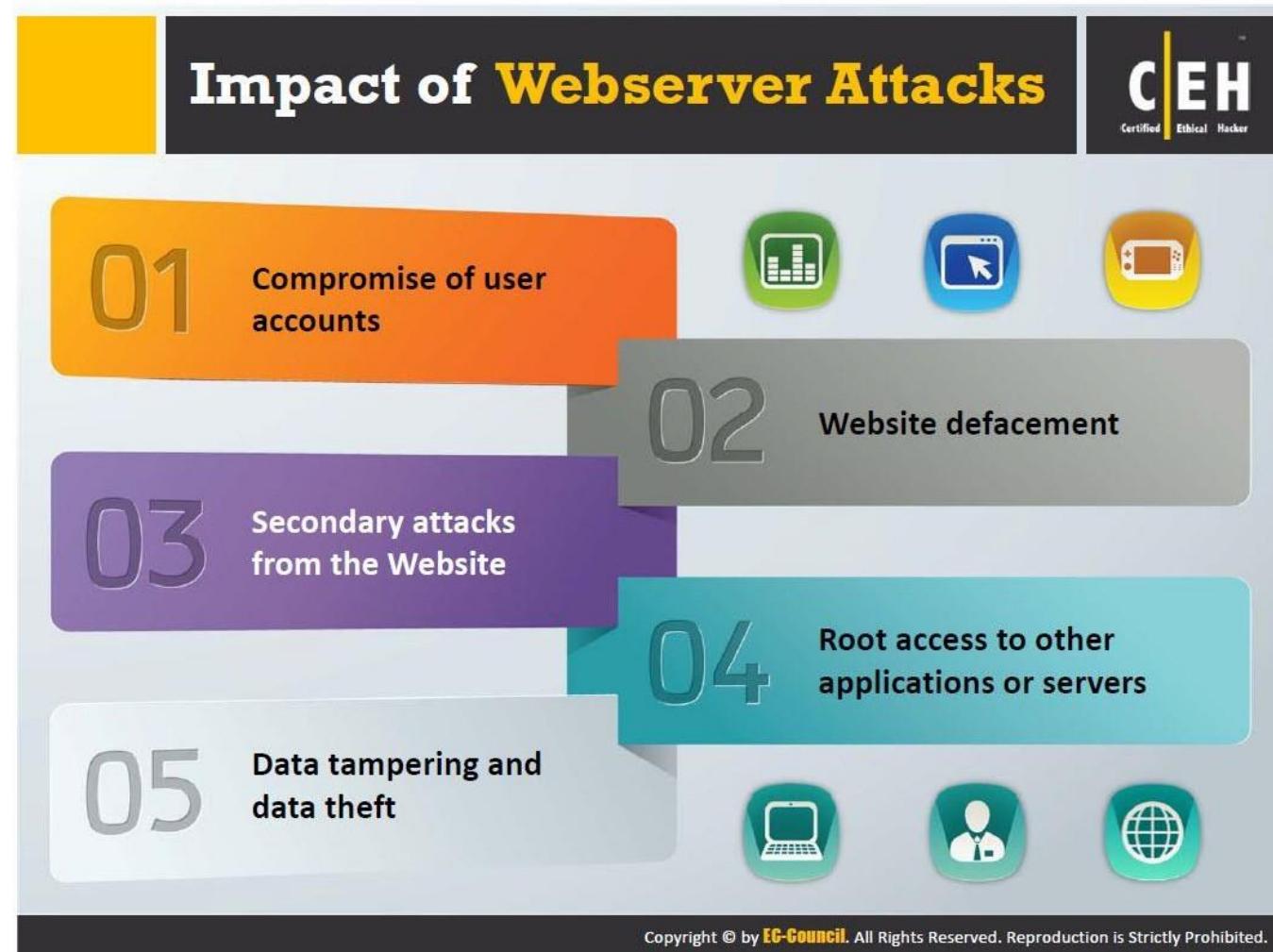
Introduction to Malware

The slide has a yellow header bar and a dark grey footer bar. The main title 'Introduction to Malware' is in white and yellow. The EC-Council Certified Ethical Hacker logo is in the top right. The central text defines malware as malicious software that damages or disables computer systems and gives limited or full control. Below is a grid of ten malware types.

Examples of Malware	
Trojan Horse	Virus
Backdoor	Worms
Rootkit	Spyware
Ransomware	Botnet
Adware	Crypter

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

Impact of Webserver Attacks



Web Application Attacks

Web Application Attacks

CEH
Certified Ethical Hacker

Vulnerabilities in **web applications** running on a webserver provide a broad attack path for webserver compromise

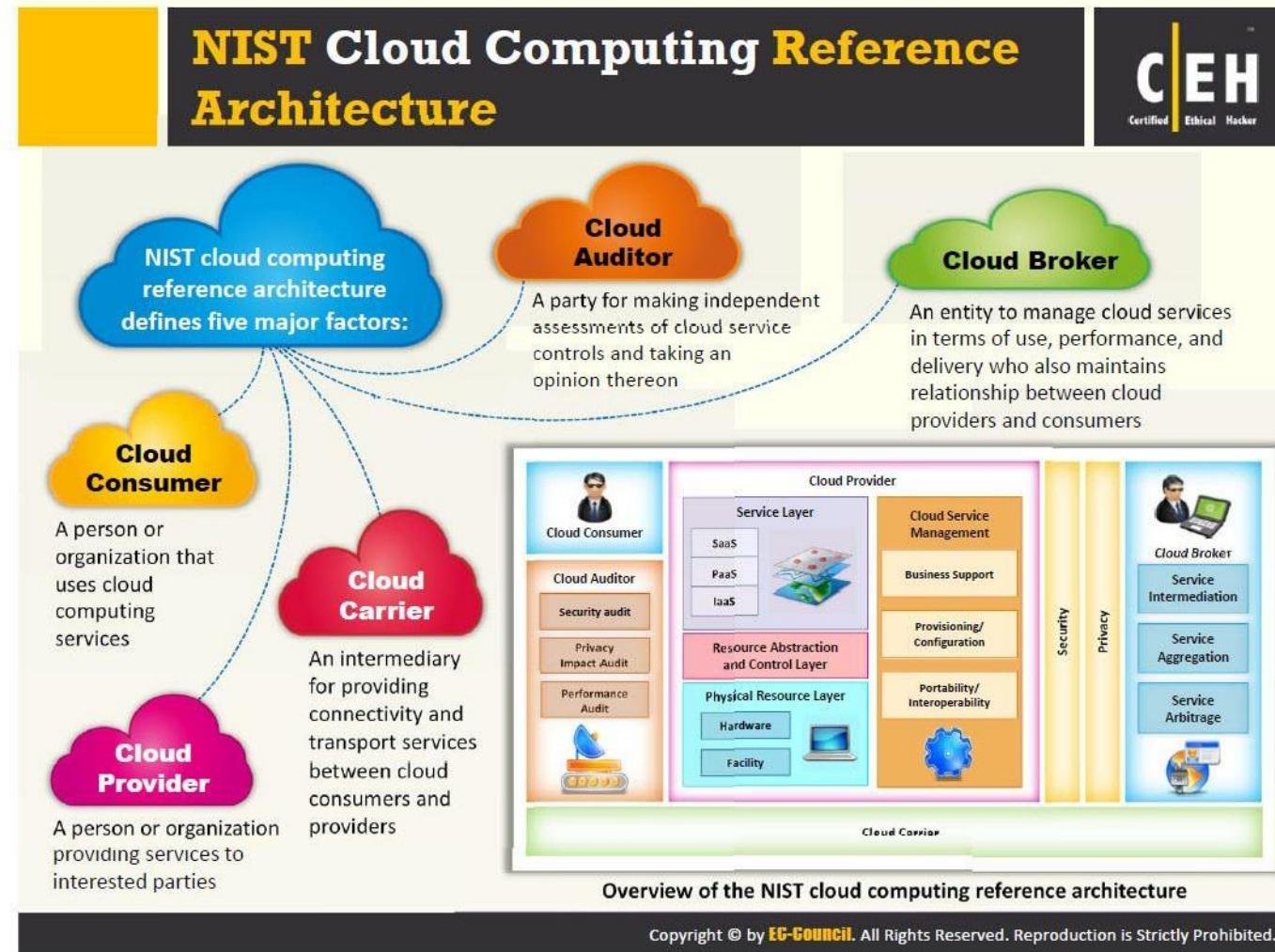


Note: For complete coverage of web application attacks refer to Module 12: Hacking Web Applications

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

Who is Responsible for my Data in the Cloud

NIST Cloud Computing Reference Architecture





Cloud Computing Attacks

- 1 Service Hijacking using Social Engineering Attacks
- 2 Session Hijacking using XSS Attack
- 3 Domain Name System (DNS) Attacks
- 4 SQL Injection Attacks
- 5 Wrapping Attack
- 6 Service Hijacking using Network Sniffing
- 7 Session Hijacking using Session Riding
- 8 Side Channel Attacks or Cross-guest VM Breaches
- 9 Cryptanalysis Attacks
- 10 DoS and DDoS Attacks

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

Cloud Computing Threats

(Cont'd)



Inadequate Infrastructure Design and Planning

- Shortage of computing resources and/or poor network design gives rise to unacceptable **network latency** or **inability to meet agreed service levels**

Conflicts between Client Hardening Procedures and Cloud Environment

- Certain client hardening procedures may conflict with a **cloud provider's environment**, making their implementation by the client impossible

Loss of Operational and Security Logs

- The loss of security logs poses a **risk for managing the implementation of the information security management program**
- Loss of security logs may occur in case of under-provisioning of storage

Malicious Insiders

- Disgruntled current or former employees, contractors, or other business partners who have authorized access to cloud resources can misuse their access to compromise the **information available in the cloud**

Cloud Computing Threats



- | | | |
|--|---|--|
| 1. Data breach/loss | 13. Loss of business reputation due to co-tenant activities | 25. Licensing risks |
| 2. Abuse of cloud services | 14. Natural disasters | 26. Loss of governance |
| 3. Insecure interfaces and APIs | 15. Hardware failure | 27. Loss of encryption keys |
| 4. Insufficient due diligence | 16. Supply chain failure | 28. Risks from changes of Jurisdiction |
| 5. Shared technology issues | 17. Modifying network traffic | 29. Undertaking malicious probes or scans |
| 6. Unknown risk profile | 18. Isolation failure | 30. Theft of computer equipment |
| 7. Inadequate infrastructure design and planning | 19. Cloud provider acquisition | 31. Cloud service termination or failure |
| 8. Conflicts between client hardening procedures and cloud environment | 20. Management interface compromise | 32. Subpoena and e-discovery |
| 9. Loss of operational and security logs | 21. Network management failure | 33. Improper data handling and disposal |
| 10. Malicious insiders | 22. Authentication attacks | 34. Loss or modification of backup data |
| 11. Illegal access to cloud systems | 23. VM-level attacks | 35. Compliance risks |
| 12. Privilege escalation | 24. Lock-in | 36. Economic Denial of Sustainability (EDOS) |

Vulnerability Assessments & Penetration Testing

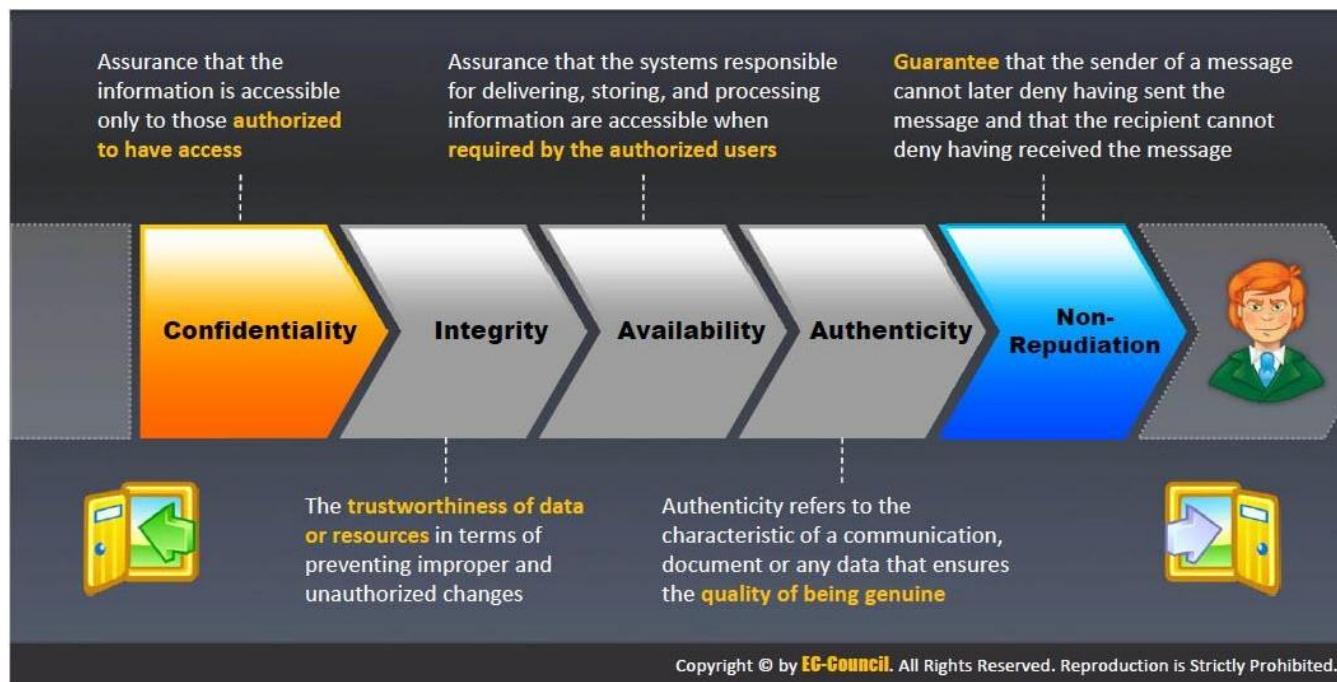




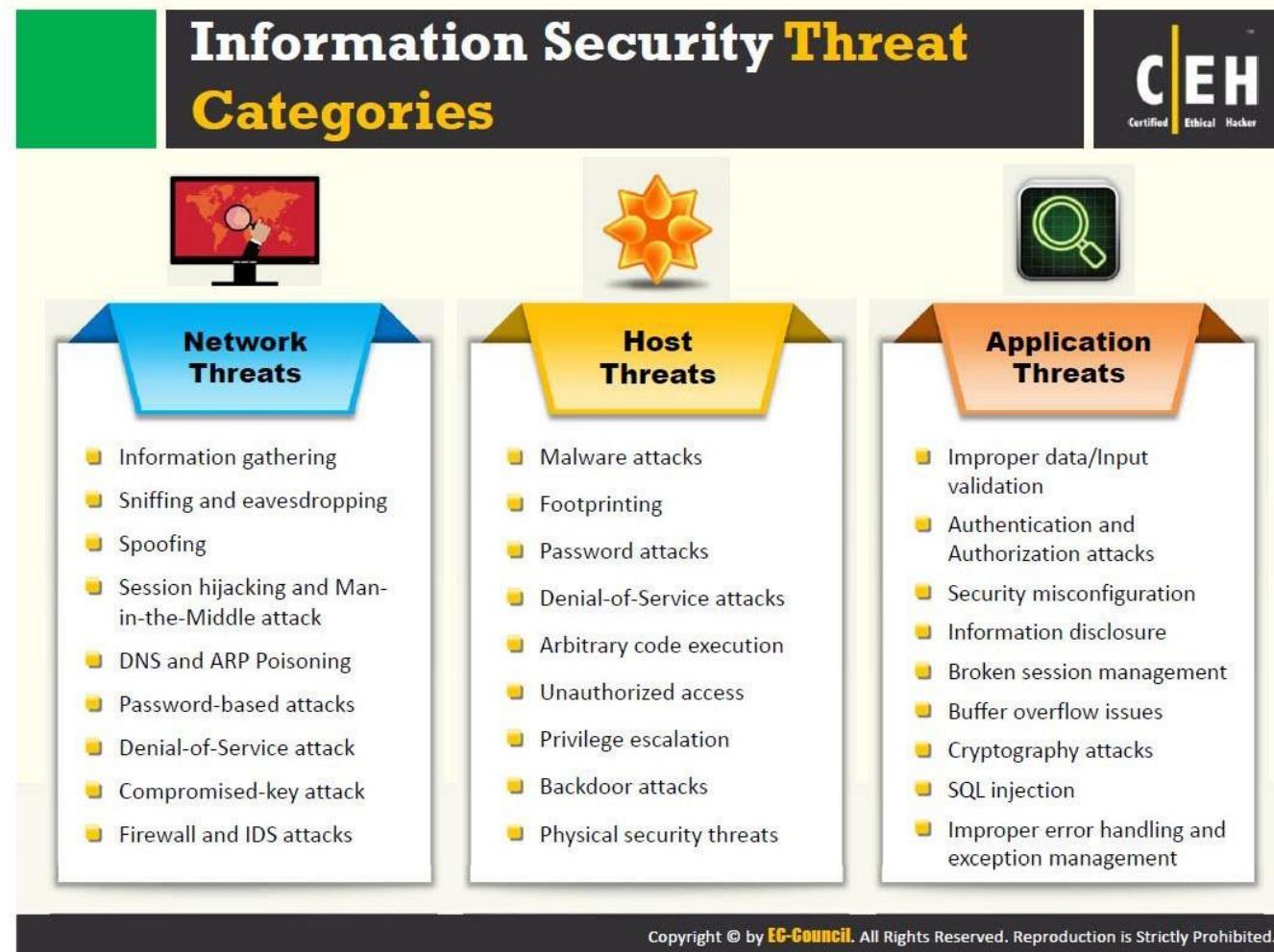
Elements of Information Security



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



Information Security Threat Categories



What is Vulnerability Assessment?

What is Vulnerability Assessment?

C|EH
Certified Ethical Hacker

Vulnerability assessment is an **examination of the ability of a system or application**, including current security procedures and controls, to withstand assault

It recognizes, measures, and classifies security vulnerabilities in a **computer system, network, and communication channels**

A vulnerability assessment may be used to:

- Identify weaknesses that could be exploited**
- Predict the effectiveness of additional security measures in protecting information resources from attack**

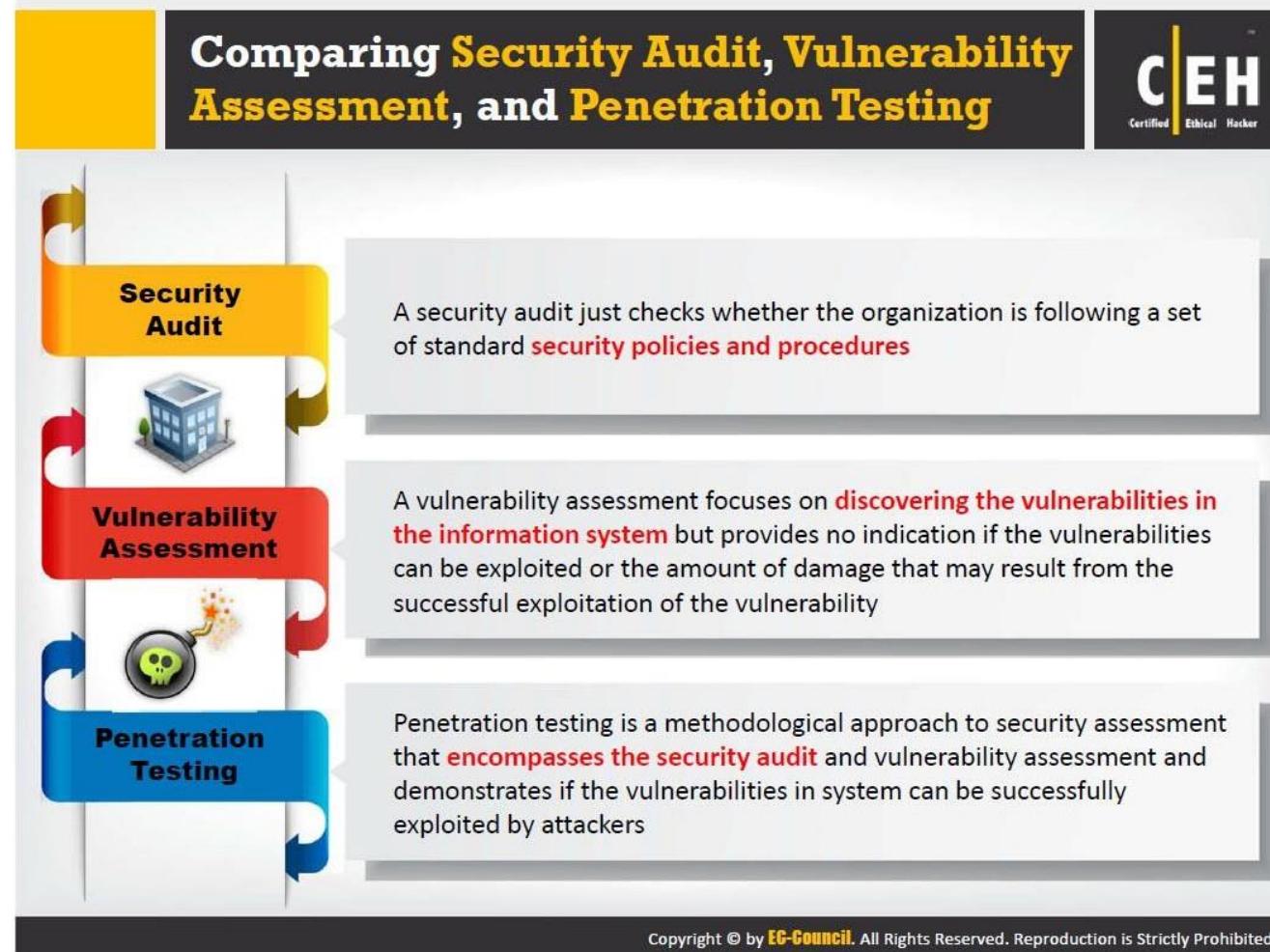
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

The infographic is titled "Penetration Testing" in large yellow text on a dark header bar. In the top right corner of the header is the "CEH" logo with the text "Certified Ethical Hacker". The main content area is divided into four horizontal sections, each with a numbered callout (01, 02, 03, 04) on the left and a corresponding icon on the right.

- 01**: Penetration testing is a method of evaluating the security of an information system or network by **simulating an attack to find out vulnerabilities** that an attacker could exploit. Icon: Person and lightbulb.
- 02**: **Security measures** are actively analyzed for design weaknesses, technical flaws and vulnerabilities. Icon: Person and Wi-Fi signal.
- 03**: A penetration test will not only point out vulnerabilities, but will also **document** how the weaknesses can be exploited. Icon: Person at desk and globe.
- 04**: The results are delivered comprehensively in a **report**, to executive management and technical audiences. Icon: Person holding a tablet and a megaphone.

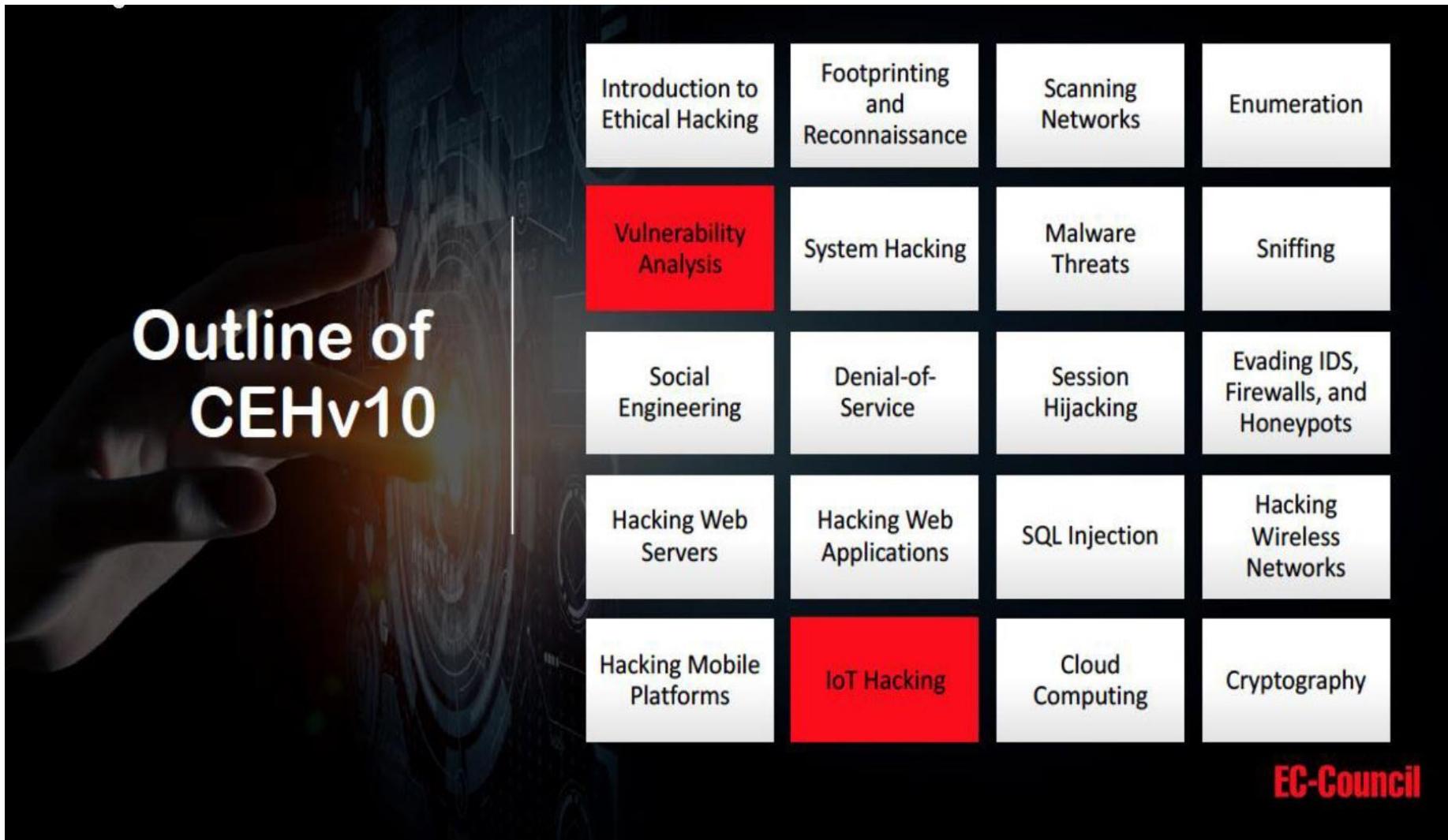
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Security Audit vs Vulnerability Assessment vs Penetration Testing



What is in the Course

Outline



New Features

Key New Features of CEHv10

Content
Malware and Attack
Vectors
Tools
Examples and Case-
studies

Inclusion New Modules –
Vulnerability Analysis

Inclusion New Modules – IoT
Hacking

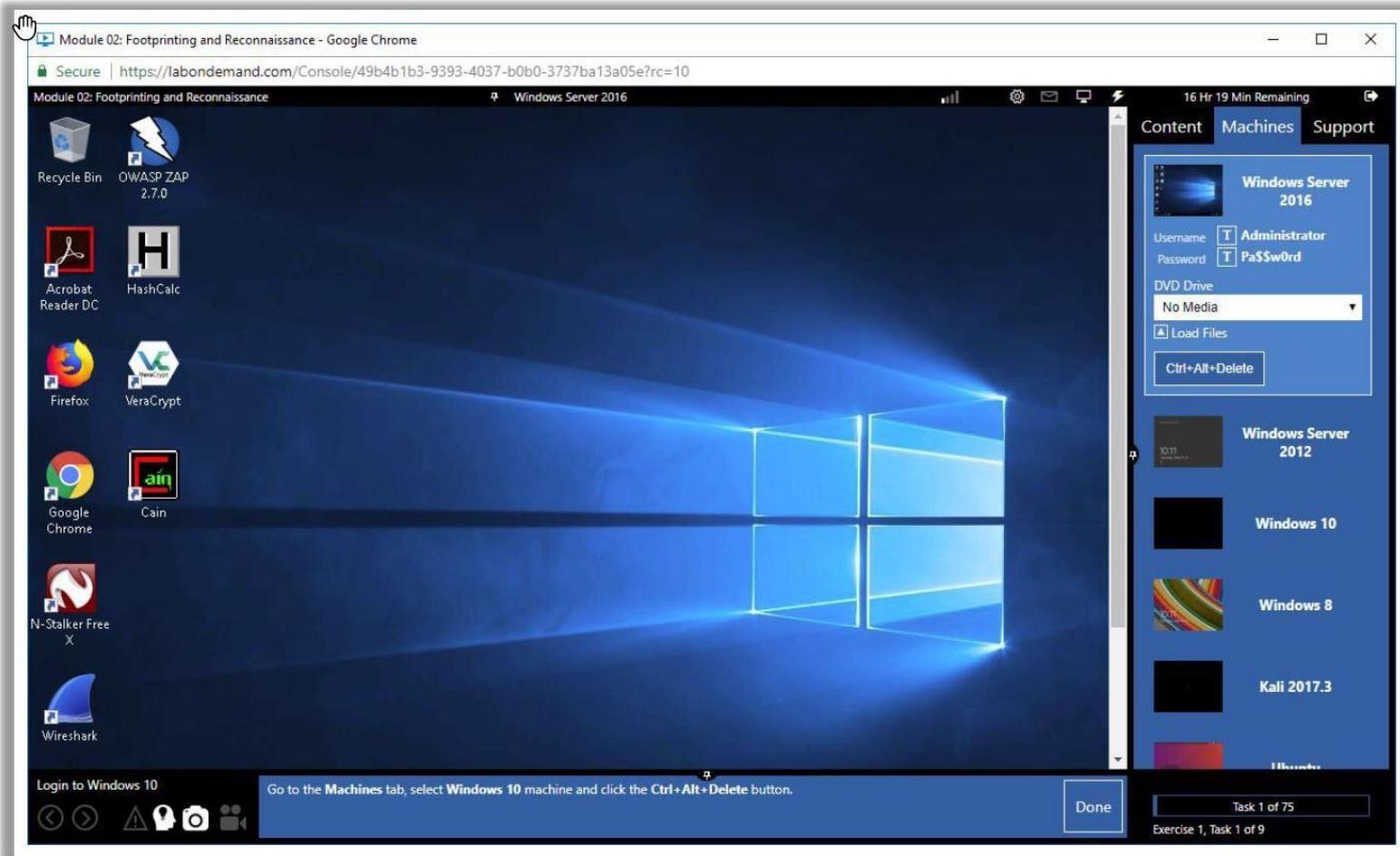
100% Compliance to NICE 2.0
Framework

Inclusion of complete Malware
Analysis Process

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

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

Windows Server 2016 Machine in iLabs



CEH Practical Credential



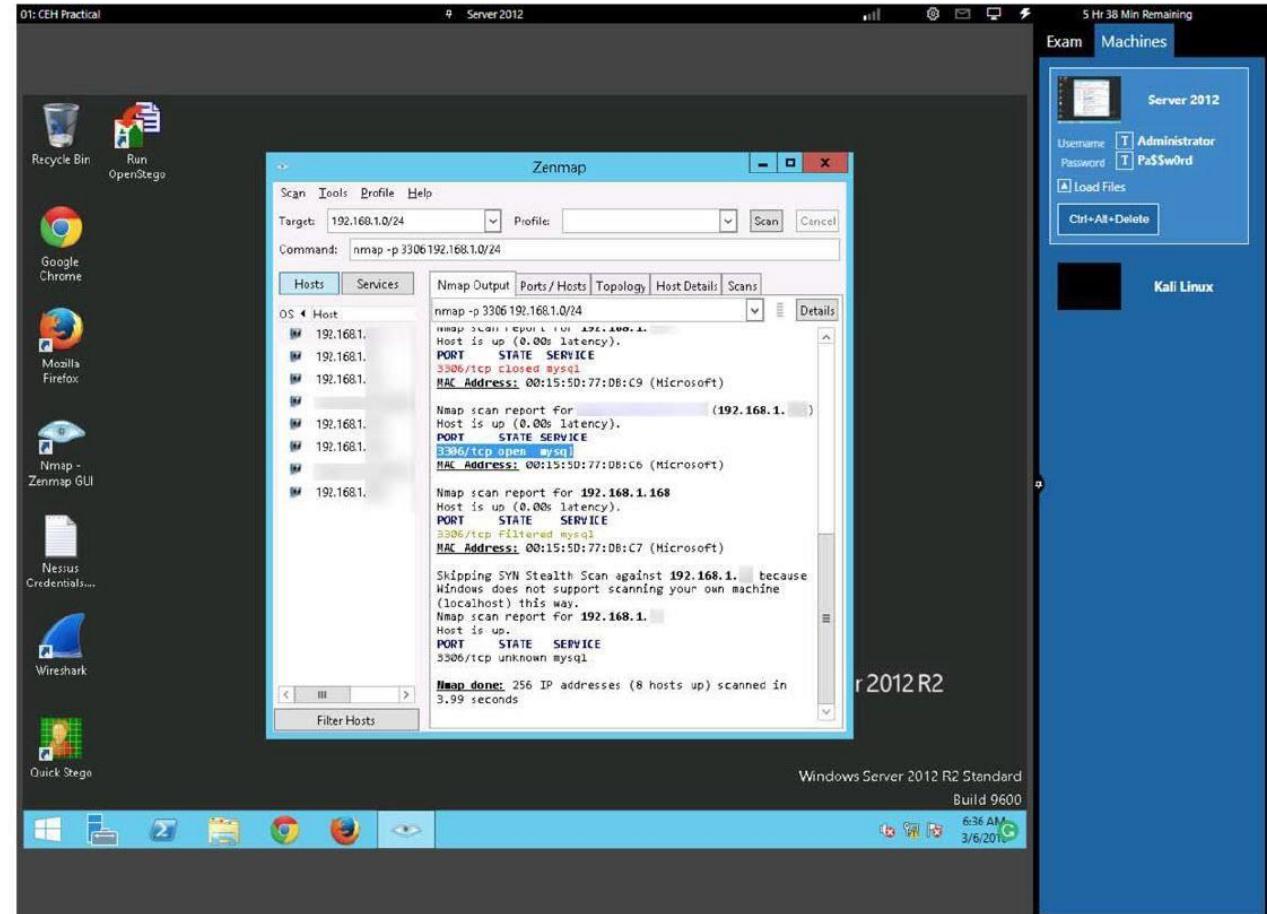
- ❖ CEH Practical EXAM is a 6 hours practical exam
- ❖ 20 real-life scenarios that requires them to demonstrate the application of ethical hacking techniques
- ❖ Remote online proctored

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!!!

