

Seguridad Web

Unidad II

2.1 Riesgo

- **Activo:** Todo recurso ya sea tangible o intangible con valor para un individuo u organización.
- **Vulnerabilidad:** **Debilidad** en el diseño, arquitectura o modo de funcionamiento de un componente.
- **Amenaza:** Entidad capaz de explotar una vulnerabilidad para aprovecharla.
- **Ataque (Exploit):** Escenario en el que una o varias amenazas explotan una vulnerabilidad.
- **Riesgo:** Probabilidad de que una o varias amenazas exploten una vulnerabilidad.
- **Impacto:** Grado de afectación debido a un ataque o exploit.



2.1 Riesgo

- Las vulnerabilidades se listan en bases de datos:
 - CVE (Common vulnerabilities and Exposures)
 - NVD (National Vulnerability Database)
 - OSV (Open Source Vulnerabilities)
 - CWE (Common Weakness Enumeration)
 - Bugtraq



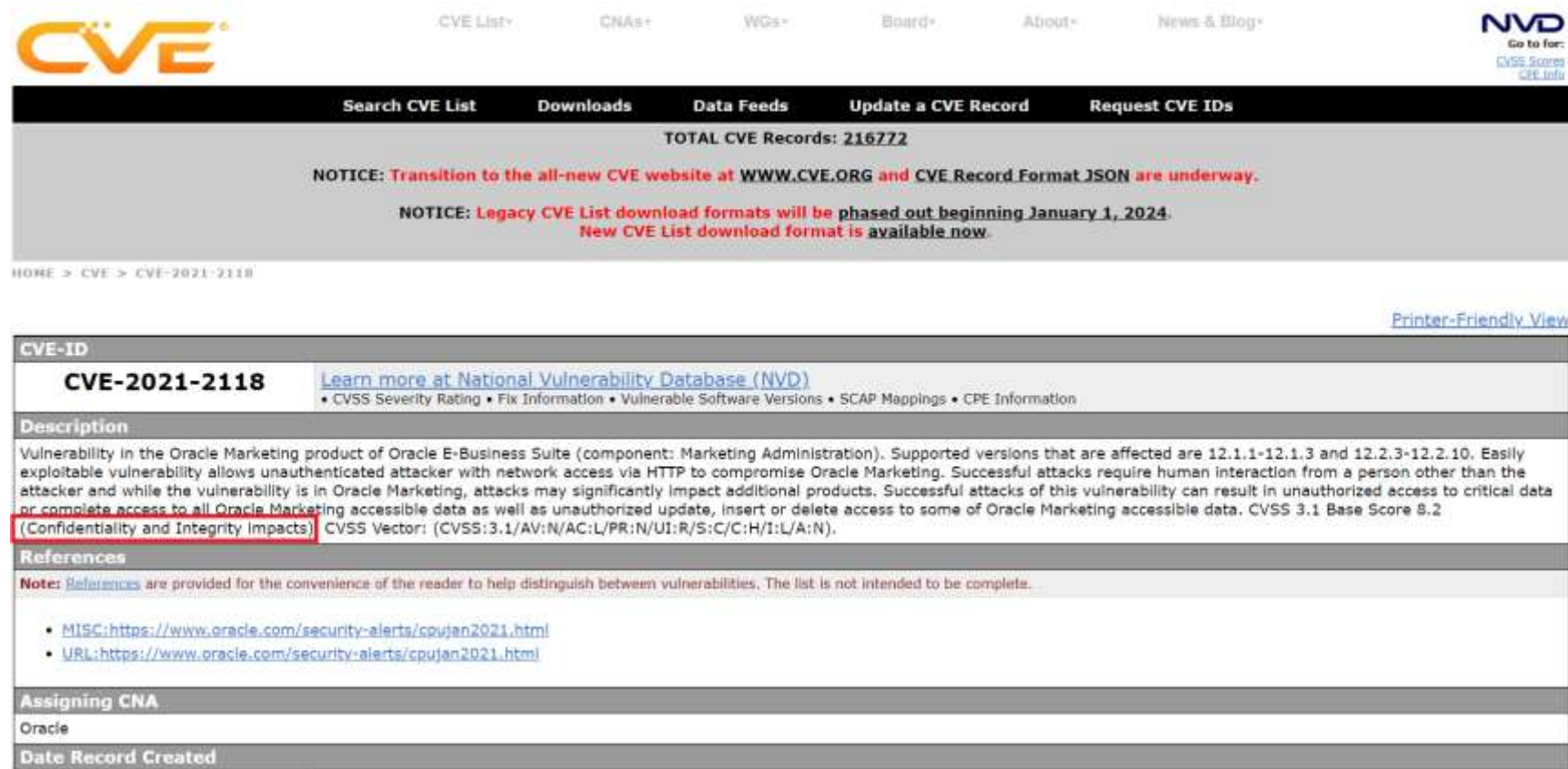
2.1 Riesgo

- Tarea 1: CVE
- Identificar de la base de datos CVE tres vulnerabilidades de cualquier dominio y describir cada uno en una ficha técnica identificando el código y el principio de seguridad de la información que afecta.



The screenshot displays the CVE website interface. At the top, there's a navigation bar with links like 'CVE List', 'CVEs', 'VDS', 'Search', 'About', and 'News & Blog'. Below this is a search bar and a 'TOTAL CVE Records: 216772' indicator. A notice states: 'NOTICE: Transition to the all-new CVE website at WWW.CVE.ORG and CVE Record Format 2.0 are underway. NOTICE: Legacy CVE List download formats will be phased out beginning January 1, 2024. New CVE List download format is available now.' The main content area shows the details for CVE-2023-21851. It includes a 'Description' section stating: 'Vulnerability in the Oracle Marketing product of Oracle E-Business Suite (component: Marketing Administration). Supported versions that are affected are 12.2.3-12.2.12. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Marketing. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Marketing accessible data. CVSS 3.1 Base Score 7.5 (Integrity impacts) CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N)'. The 'References' section lists: '• [NSIC/Oracle Advisory](#)' and '• [URL: https://www.oracle.com/security-alerts/cve2023.html](https://www.oracle.com/security-alerts/cve2023.html)'. The 'Assigning CNA' is listed as 'Oracle'. The 'Date Record Created' is '20221217'. A disclaimer at the bottom states: 'Disclaimer: The record creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.'

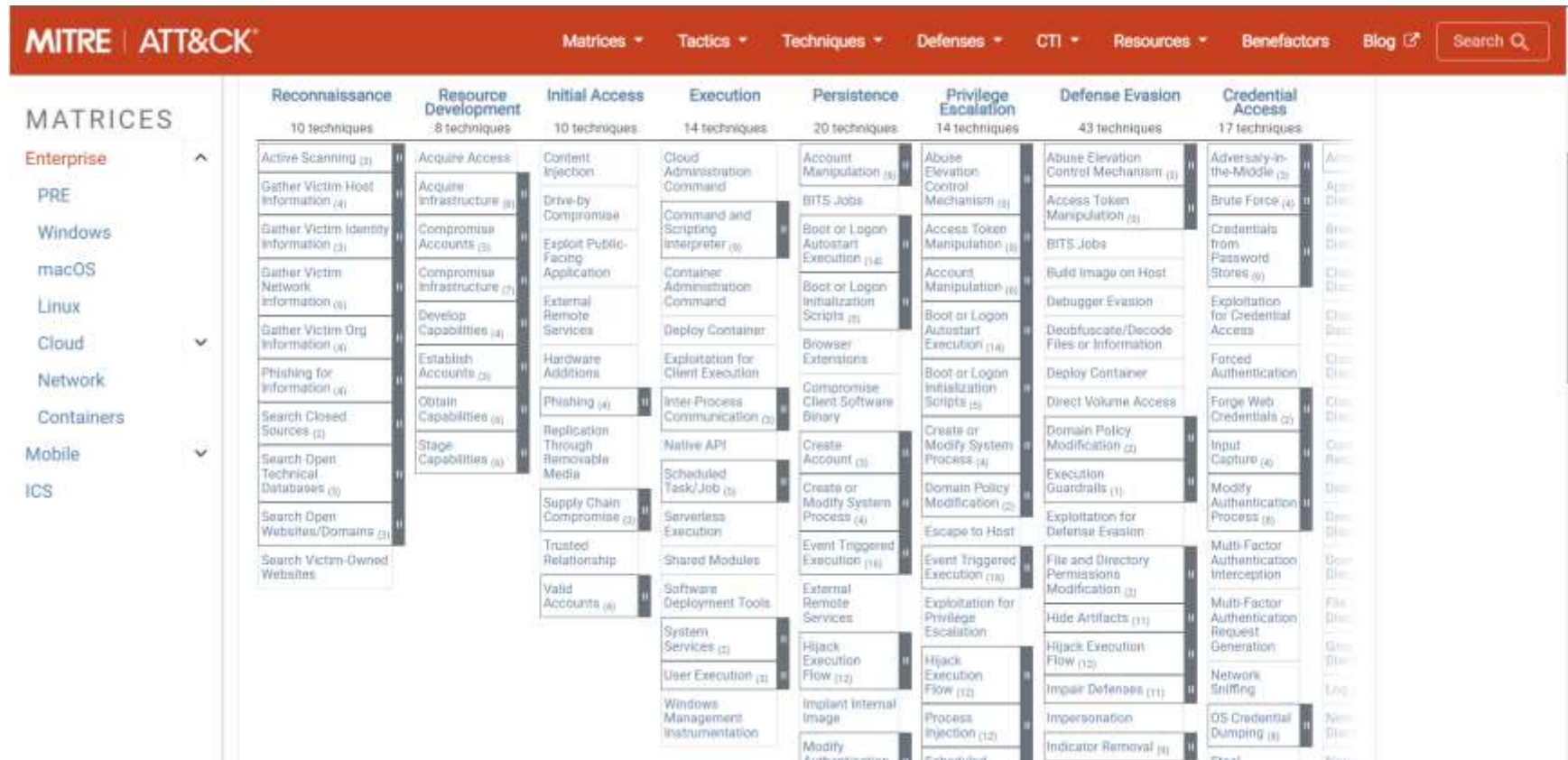
2.1 Riesgo



The screenshot shows the CVE website interface. At the top, there's a navigation bar with links like 'CVE List', 'CNAs', 'WGs', 'Board', 'About', and 'News & Blog'. Below this is a search bar and a 'Go to for: CVE Scores CVE Info' link. The main content area displays 'TOTAL CVE Records: 216772' and a notice about the transition to the new CVE website at WWW.CVE.ORG. Below the notice, there's a breadcrumb trail: 'HOME > CVE > CVE-2021-2118'. The main entry for CVE-2021-2118 is shown, including a link to 'Learn more at National Vulnerability Database (NVD)' and a list of links: 'CVSS Severity Rating', 'Fix Information', 'Vulnerable Software Versions', 'SCAP Mappings', and 'CPE Information'. The 'Description' section states: 'Vulnerability in the Oracle Marketing product of Oracle E-Business Suite (component: Marketing Administration). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Marketing. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Marketing, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Marketing accessible data as well as unauthorized update, insert or delete access to some of Oracle Marketing accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity Impacts)'. The 'References' section includes a note: 'Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.' and two links: 'MISC: https://www.oracle.com/security-alerts/cpujan2021.html' and 'URL: https://www.oracle.com/security-alerts/cpujan2021.html'. The 'Assigning CNA' section lists 'Oracle' and the 'Date Record Created' is shown at the bottom.

2.1 Riesgo

- Los ataques contra las amenazas pueden ser encontrados en el MITRE ATT&CK.

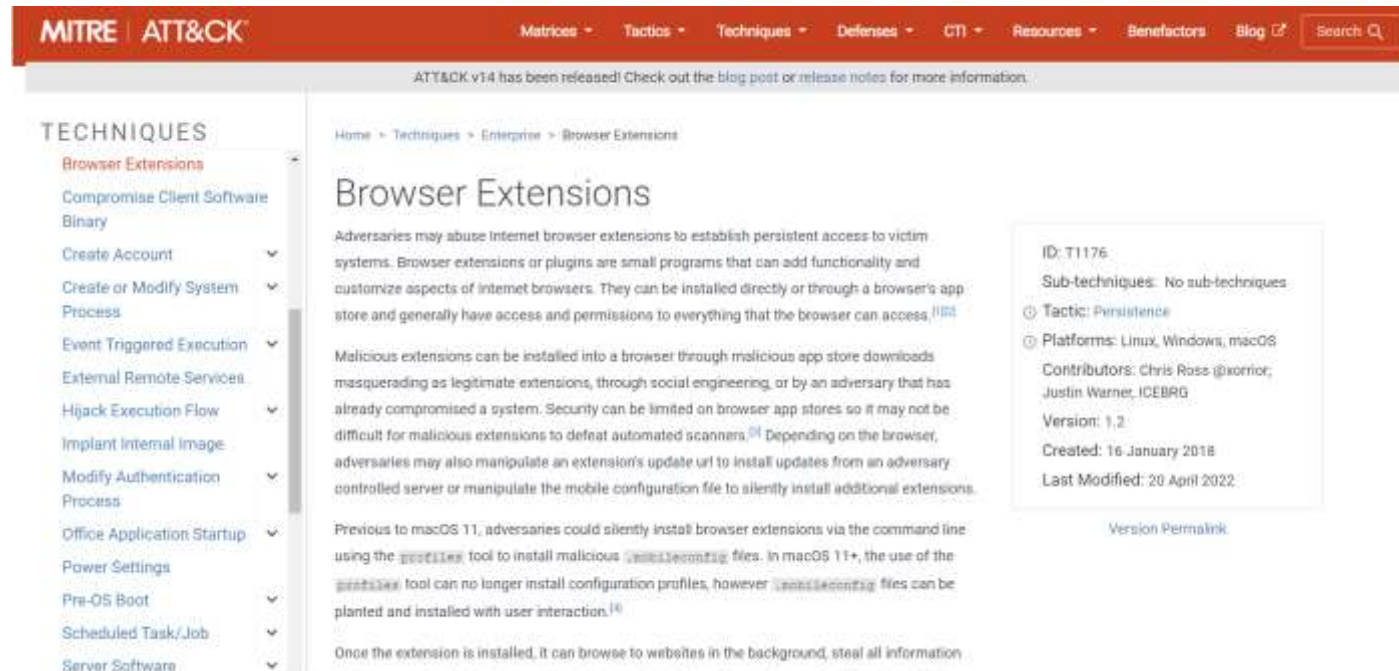


The screenshot displays the MITRE ATT&CK framework interface. The top navigation bar includes links for Matrices, Tactics, Techniques, Defenses, CTI, Resources, Benefactors, and a Blog. A search bar is also present. The main content area is divided into several columns representing different attack phases: Reconnaissance (10 techniques), Resource Development (8 techniques), Initial Access (10 techniques), Execution (14 techniques), Persistence (20 techniques), Privilege Escalation (14 techniques), Defense Evasion (43 techniques), and Credential Access (17 techniques). On the left side, there is a sidebar titled 'MATRICES' with a list of operating systems and environments: Enterprise, PRE, Windows, macOS, Linux, Cloud, Network, Containers, Mobile, and ICS. The 'Enterprise' matrix is currently selected, showing a grid of specific attack techniques categorized by the phases mentioned above.

2.1 Riesgo

- **Tarea 2: MITRE ATT&CK**
- Identificar tres ataques en el dominio Enterprise y construir una ficha técnica de cada ataque.

- ID
- Procedure
- Mitigations
- Detection



The screenshot shows the MITRE ATT&CK website. The top navigation bar includes links for Matrices, Tactics, Techniques, Defenses, CTF, Resources, Benefactors, and a Blog. A search bar is also present. Below the navigation bar, a banner announces 'ATT&CK v14 has been released!'. The main content area is titled 'Browser Extensions' and describes how adversaries can abuse browser extensions for persistent access. A sidebar on the left lists various techniques under the 'TECHNIQUES' heading. On the right, a box provides technical details for the 'T1176' technique, including its tactic (Persistence), platforms (Linux, Windows, macOS), contributors, version, creation date, and last modification date.

MITRE ATT&CK

Matrices - Tactics - Techniques - Defenses - CTF - Resources - Benefactors - Blog

ATT&CK v14 has been released! Check out the [blog post](#) or [release notes](#) for more information.

TECHNIQUES

- Browser Extensions
- Compromise Client Software Binary
- Create Account
- Create or Modify System Process
- Event Triggered Execution
- External Remote Services
- Hijack Execution Flow
- Implant Internal Image
- Modify Authentication Process
- Office Application Startup
- Power Settings
- Pre-OS Boot
- Scheduled Task/Job
- Server Software

Home > Techniques > Enterprise > Browser Extensions

Browser Extensions

Adversaries may abuse Internet browser extensions to establish persistent access to victim systems. Browser extensions or plugins are small programs that can add functionality and customize aspects of Internet browsers. They can be installed directly or through a browser's app store and generally have access and permissions to everything that the browser can access.^{[1][2]}

Malicious extensions can be installed into a browser through malicious app store downloads masquerading as legitimate extensions, through social engineering, or by an adversary that has already compromised a system. Security can be limited on browser app stores so it may not be difficult for malicious extensions to defeat automated scanners.^[3] Depending on the browser, adversaries may also manipulate an extension's update url to install updates from an adversary controlled server or manipulate the mobile configuration file to silently install additional extensions.

Previous to macOS 11, adversaries could silently install browser extensions via the command line using the `profiles` tool to install malicious `mobileconfig` files. In macOS 11+, the use of the `profiles` tool can no longer install configuration profiles, however `mobileconfig` files can be planted and installed with user interaction.^[4]

Once the extension is installed, it can browse to websites in the background, steal all information

ID: T1176
Sub-techniques: No sub-techniques
Tactic: Persistence
Platforms: Linux, Windows, macOS
Contributors: Chris Ross (@xorrior), Justin Warner, ICEBRG
Version: 1.2
Created: 16 January 2018
Last Modified: 20 April 2022

[Version](#) [Permalink](#)

2.2 Controles y Riesgo Residual

- **Control:** Medida de protección para mitigar el riesgo inherente por la presencia de amenazas.
 - Firewalls
 - Cifrado
 - CAPTCHAs
 - Hash
- **Riesgo residual:** Riesgo resultante después de la aplicación de uno o varios controles.



2.2 Controles y Riesgo Residual

Ejemplo de matriz de riesgo 5x5

Impacto
¿Qué tan severos serían los resultados si ocurriera el riesgo?

Probabilidad
¿Cuál es la probabilidad de que ocurra el riesgo?

	Insignificante 1	Menor 2	Significativo 3	Mayor 4	Severo 5
5 Casi seguro	Medio 5	Alto 10	Muy alto 15	Extremo 20	Extremo 25
4 Probable	Medio 4	Medio 8	Alto 12	Muy alto 16	Extremo 20
3 Moderado	Bajo 3	Medio 6	Medio 9	Alto 12	Muy alto 15
2 Poco probable	Muy bajo 2	Bajo 4	Medio 6	Medio 8	Alto 10
1 Raro	Muy bajo 1	Muy bajo 2	Bajo 3	Medio 4	Medio 5

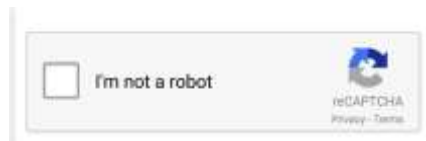
SafetyCulture

ESTRATEGIAS PARA EL TRATAMIENTO DE RIESGOS



2.3 Mecanismos de Protección: CAPTCHA

- **Completely Automated Public Turing test to tell Computers and Humans Apart.**
- Comprende un control de protección contra bots y web crawlers: amenazas automatizadas.
- Presenta desafíos visuales o cognitivos fáciles de resolver para un humano pero complejos para una máquina:
 - Selección de imágenes.
 - Resolución de recompecabezas de texto.
 - Resolución de operaciones matemáticas simples.
 - Identificación de objetos.
 - Completar la secuencia de textos o números.



2.4 Mecanismos de Protección: Hashing

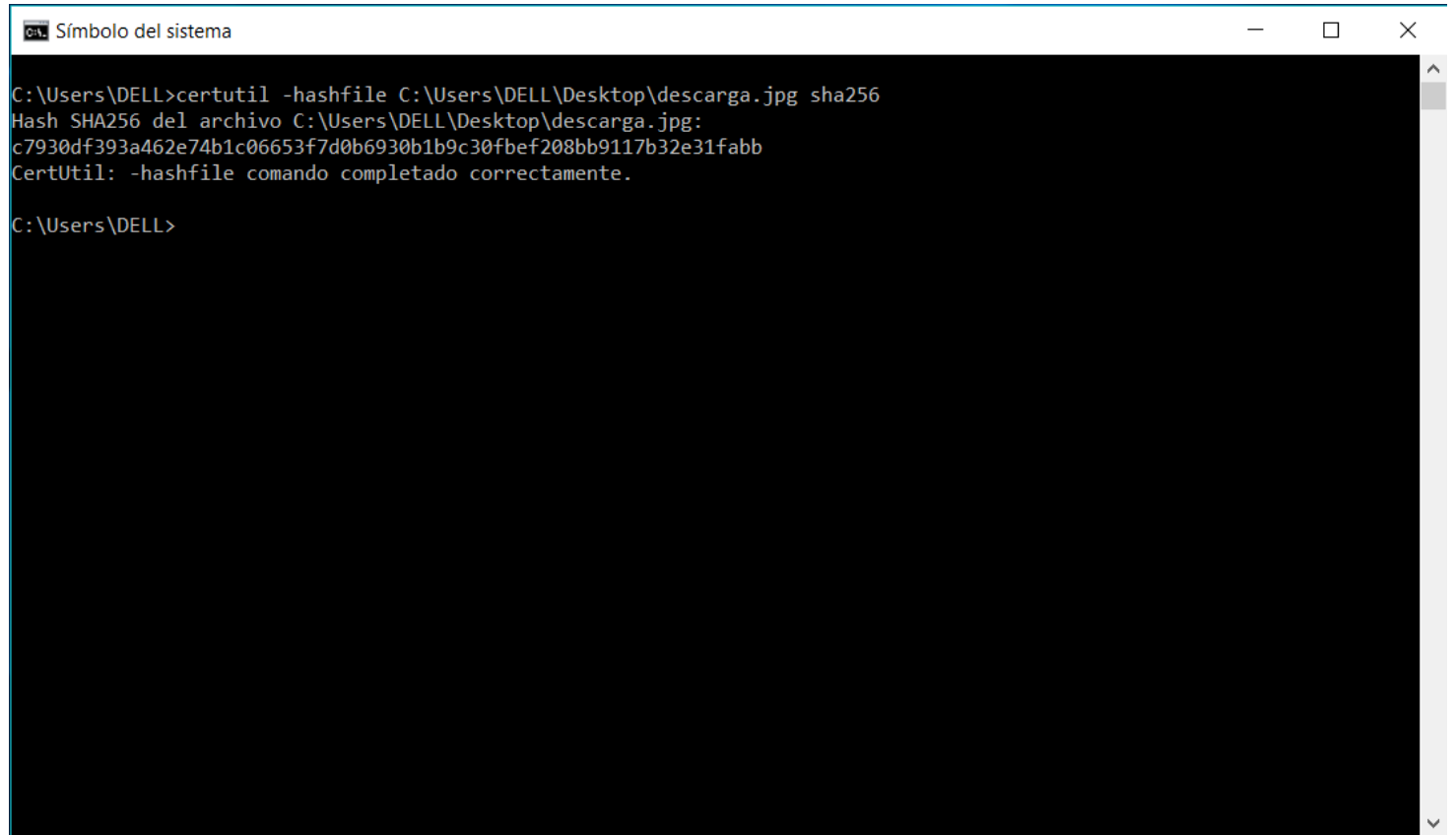
- Mecanismo de protección para precautelar la integridad.
- Varios algoritmos:
 - MD5
 - SHA-1
 - SHA-2
 - SHA-3
- Cada algoritmo genera una salida de un determinado número de bits.
 - MD5 -> 128 bits (32 caracteres hexadecimales)
 - SHA-1 -> 160 bits (40 caracteres hexadecimales)



2.4 Mecanismos de Protección: Hashing

Calculando hashes en Windows:

certutil -hashfile <file> <algorithm>

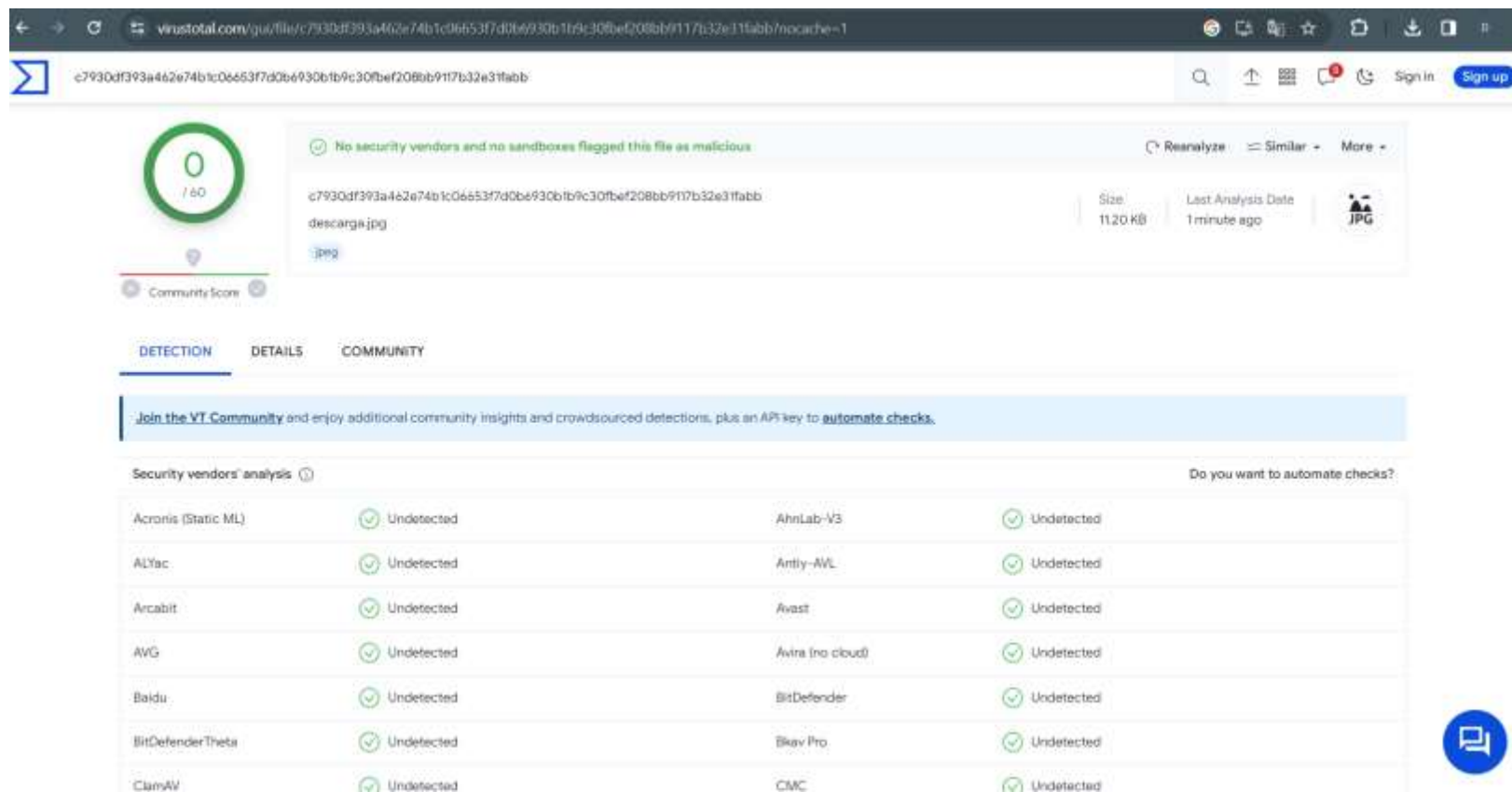


```
Símbolo del sistema

C:\Users\DELL>certutil -hashfile C:\Users\DELL\Desktop\descarga.jpg sha256
Hash SHA256 del archivo C:\Users\DELL\Desktop\descarga.jpg:
c7930df393a462e74b1c06653f7d0b6930b1b9c30fbef208bb9117b32e31fabb
CertUtil: -hashfile comando completado correctamente.

C:\Users\DELL>
```

2.4 Mecanismos de Protección: Hashing



File Hash: e7930df393a462e74b1c06653f7d0b6930b1b9c30fbef208bb9117b32e31fabbb

File Name: descarga.jpg

Size: 11.20 KB

Last Analysis Date: 1 minute ago

Community Score: 0

Security vendors' analysis:

Vendor	Result	Vendor	Result
Acronis (Static ML)	Undetected	AhnLab-V3	Undetected
ALYac	Undetected	Antiy-AVL	Undetected
Arcabit	Undetected	Avast	Undetected
AVG	Undetected	Avira (no cloud)	Undetected
Baidu	Undetected	BitDefender	Undetected
BitDefenderTheta	Undetected	Bkav Pro	Undetected
ClamAV	Undetected	CMC	Undetected

2.4 Mecanismos de Protección: Hashing

```
import hashlib

texto = "Curso de Seguridad Web:"

hash = hashlib.sha1()
hash.update(texto.encode())
hash.hexdigest()

'b23d4140381eabe4dd849c6a7a127e914201e2d9'
```



2.5 Mecanismos de Protección: Cifrado simétrico

- También llamado cifrado de clave privada (o llave privada).
- Emplea la misma clave para cifrar y para descifrar.
- El secreto de la clave comprende la fortaleza del método de cifrado, pero no así el algoritmo por sí mismo.
- Por lo tanto la clave ser fuerte y dinámica.
- Algoritmos:
 - Fernet
 - AES
 - Blowfish
 - DES
 - 3DES
 - RC6
 - RC5
 - RC4



2.5 Mecanismos de Protección: Cifrado simétrico



2.5 Mecanismos de Protección: Cifrado simétrico

```
from cryptography.fernet import Fernet
```

```
clave = Fernet.generate_key()  
cipher_suite = Fernet(clave)  
print(clave)
```

```
texto_original = "Este es un mensaje secreto"  
texto_bytes = texto_original.encode()  
texto_cifrado = cipher_suite.encrypt(texto_bytes)
```

```
print("Texto cifrado:", texto_cifrado)
```

```
b'U2PuHGcqeDXGoJ4yvMpRc_Lf_QAr3-IJQyO-9kkKUIU='
```

```
Texto cifrado: b'gAAAAABlV5IIHSH70-MchdMqzuzgWajpmROF27AyyDTrYn7d_YzH02p0UDH2z2DLRfUfSFWvSbKLYBt19XTk6_1KrTymisEUhEatVXtEKeTZmHlagnArq74='
```



2.5 Mecanismos de Protección: Cifrado simétrico

```
clave = b'U2PuHGcqeDXGoJ4yvMpRc_Lf_QAr3-IJQy0-9kkKUIU='  
cipher_suite = Fernet(clave)  
texto_descifrado = cipher_suite.decrypt(texto_cifrado)  
texto_claro = texto_descifrado.decode()  
  
print("Texto descifrado:", texto_descifrado)
```

Texto descifrado: b'Este es un mensaje secreto'

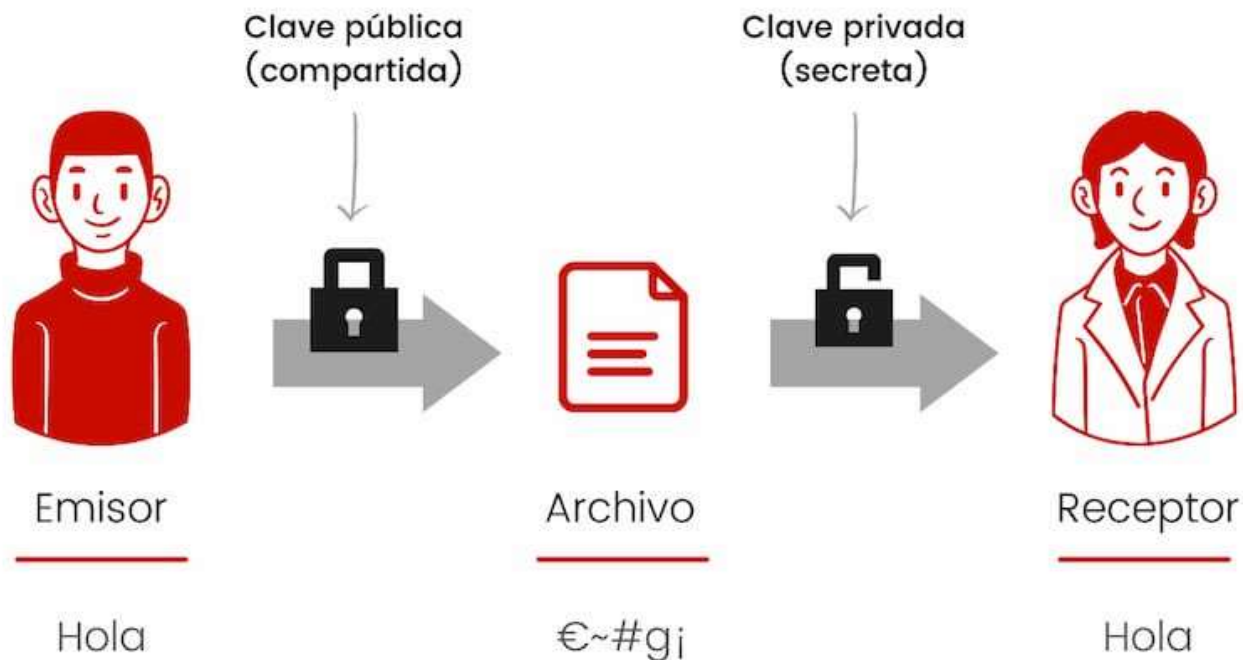


2.6 Mecanismos de Protección: Cifrado asimétrico

- También llamado cifrado de clave pública (o llave pública).
- Se emplean dos claves: una pública y una privada.
- Algoritmos:
 - RSA
 - ElGamal
 - ECDSA (Elliptic Curve Digital Signature Algorithm)



2.6 Mecanismos de Protección: Cifrado asimétrico



ATICO34



2.6 Mecanismos de Protección: Firma digital

- Mecanismo para precautelar: Autenticación, Integridad y No repudio.
- Comprende un hash cifrado con la clave privada del emisor.
- Entonces se valida la identidad del emisor pues la firma se puede decifrar con su clave pública por cualquier entidad.
- Ampliamente utilizado en **comercio electrónico**.



2.6 Mecanismos de Protección: Firma digital

