Punto de control: Resultado

Estimado/a alumno/a:

Una vez iniciado el practico no podrá detenerse y deberá concluirse antes el tiempo indicado.

Cuando responda todas la preguntas, presione el botón de FINALIZAR EXAMEN en la parte inferior. No recargue la página ni presione hacia atrás en el navegador, de lo contrario su examen quedará invalidado.

Ante cualquier problema indíqueselo al docente a cargo.

Trabajos Prácticos de Respuesta Múltiple N°8 P2 - CORRECTAS: 9 de 10 -

**APROBADO**

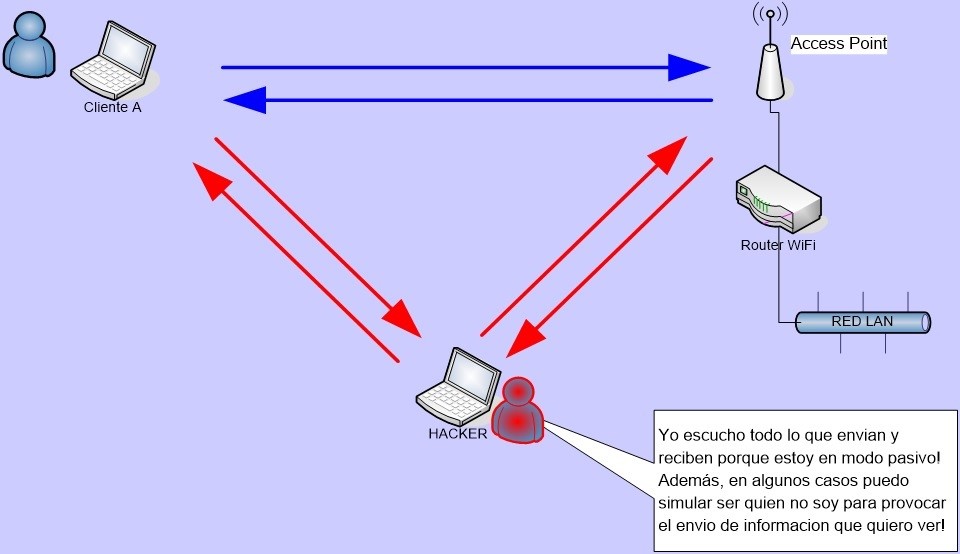
1. El software o hardware subrepticio que se encarga de registrar las pulsaciones que se realizan en elteclado, para posteriormente memorizarlas en un archivo o enviarlas a través de internet se lo denomina:



a) Keylogger.

* 1. Ramsomware.
  2. Jamming.
  3. IDS.
  4. Pharming.
  5. Ninguna de las Anteriores es correcta.

1. El tipo de ataque informático que consiste en una técnica de sni ng de paquetes circulante e inyección de datos malignos para producir determinados resultados en comunicaciones inalámbricas se lo denomina:



a) Jamming.

* 1. Pharming.
  2. Keylogger.
  3. Spoo ng.
  4. ARP Poisoning.
  5. Ramsomware.
  6. Todas las Anteriores son correctas.

h) Ninguna de las Anteriores es correcta.

1. Aquella incursión informática ilegal que tienen por objeto, el robo de datos personales de identidad einformación de credenciales nancieras; y a veces simula un sitio web para capturar datos de login con una pantalla de ingreso al sistema se la denomina:

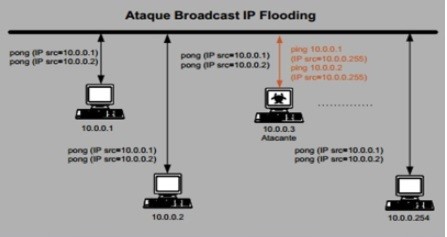


* 1. Keylogger.
  2. Ramsomware.

c) Phishing.

* 1. Flooding.
  2. Pharming.
  3. Ninguna de las Anteriores es correcta.

1. La técnica de Jamming o Flooding o inundación es una técnica que busca generar solicitudesmaliciosas a un servicio de internet con la nalidad de hacer que el mismo se sature o entre en un modo de espera, de esta forma anula o limita su funcionamiento. Dicho ataque de acuerdo con su tipo corresponde a:



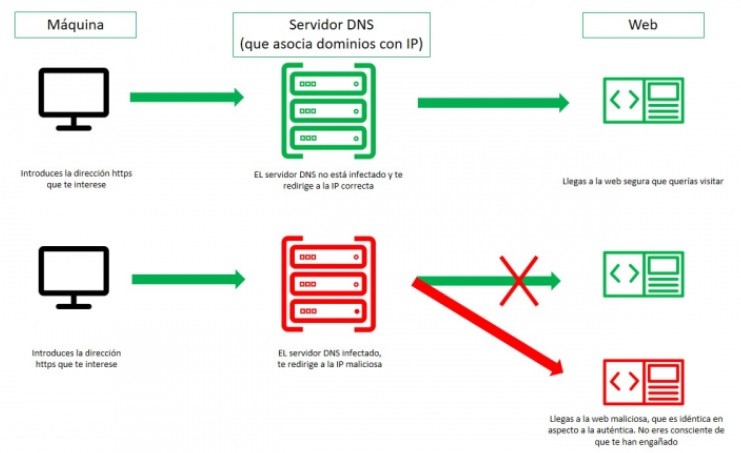
a) Fuerza Bruta

* 1. Ramsomware.

c) Denegación de Servicio

* 1. Escaneo de Puertos.
  2. Autenticación.
  3. Ninguna de las Anteriores es correcta.

1. Cuando se realiza una ciberincursión que provoca el “DNS Hijacking” y “DNS Poisoning” que consistenen la publicación ilegitima de resolución de un dominio mediante la modi cación de los registros de un servidor DNS, Dicho ataque corresponde a:

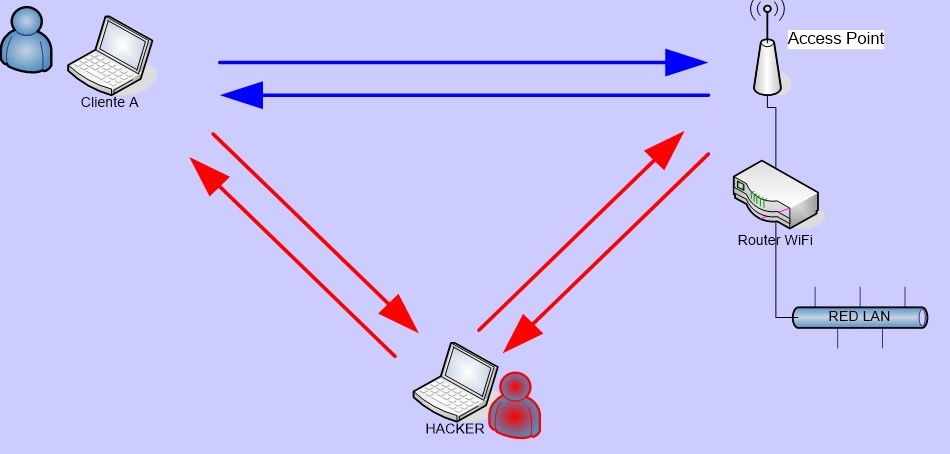


a) Jamming.

b) Pharming.

* 1. Keylogger.
  2. Man in the Midlee.
  3. ARP Poisoning.
  4. Ramsomware.
  5. Todas las Anteriores son correctas.
  6. Ninguna de las Anteriores es correcta.

1. Cuando nos referimos a MAC SPOOFING podemos a rmar que:



* 1. Es un tipo de ataque de robo de identidad.
  2. Es una técnica para clonar la dirección MAC de un dispositivo de red.
  3. Es una Técnica que se utiliza en comunicaciones inalámbricas.
  4. Es una técnica para cambiar la dirección MAC de un dispositivo de red.

e) Todas las Anteriores son Correctas.

f) Ninguna de las Anteriores es correcta.

1. Existe un tipo de peste o alimaña que funciona en su PC, sin su consentimiento o como parte de unconsentimiento genérico, habitualmente se ejecuta en background y le abre ventanas emergentes en el programa navegador en concordancia con los sitios habituales que UD. visualiza. El tipo de malware corresponde a:



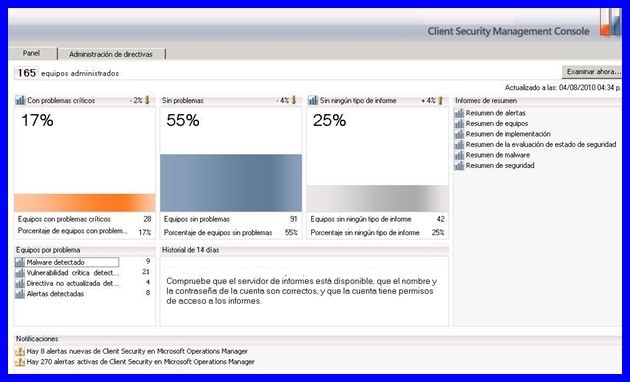
a) Virus de Macro

* 1. Gusano.
  2. Caballo de troya
  3. Virus de sector de Arranque.

e) Spyware.

f) Ninguna de las Anteriores es correcta.

1. Un Programa Antivirus dentro de un entorno de red controlado debe cumplir con las siguientesfunciones:



* 1. La prevención de ejecución de código malicioso y su replicación en memoria.
  2. La protección y bloqueo de Puertos
  3. Analizar y buscar código malicioso desde archivos hasta comunicaciones (E-mail, tra coWeb, etc.) dentro de nuestro entorno de red, servidores y terminales.
  4. Proteger con sistemas de encriptación la información a ser transportada por la red. e) Ambas a y b.

f) Ambas a y c

* 1. Ambas a y d.
  2. Ninguna de las Anteriores es correcta.

1. El Con cker (2008) era un virus que apareció en Ucrania e infectaba computadoras con sistemas

Windows PC, Server 2003 y 2008. El Malware desactivaba Servicios de Update, Windows Security Center, Sistema Antivirus Defender. A su vez bloqueaba cuentas de Usuario, inundaba ARP y volvía los controladores de dominio lentos. Usaba como modo de propagación las redes y los pendrives. El tipo de virus corresponde a:



* 1. Virus de Macro.
  2. Gusano.

c) Caballo de troya.

* 1. Virus de Arranque.
  2. Virus de Script.
  3. Ninguna de las Anteriores es correcta.

1. El Programa malicioso que restringen el acceso a determinadas partes o archivo del sistemaoperativo infectado, reteniendo el control del equipo y que encripta la información almacenada en el mismo para que no pueda ser accedida; solicitando un rescate nanciero en criptomonedas para que sean desactivados se lo denomina.



a) Jamming.

* 1. Pharming.
  2. Keylogger.
  3. Spoo ng.
  4. ARP Poisoning.

f) Ramsomware.

* 1. Todas las Anteriores son correctas.
  2. Ninguna de las Anteriores es correcta.

|  |  |  |
| --- | --- | --- |
| **RESUMEN**  Trabajos Prácticos de Respuesta Múltiple N°8  P2 | CORRECTAS: 9 de 10 | **APROBADO** |

[SALIR](https://miel.unlam.edu.ar/evaluacion/event/salir/comision/30097433)

Departamento de Ingeniería e Investigaciones Tecnológicas - Materias Interactivas en

Línea - 2023