

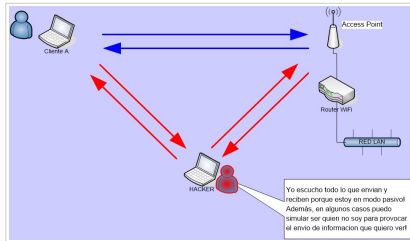
Evaluación

Evaluaciones

Punto de control: Resultado

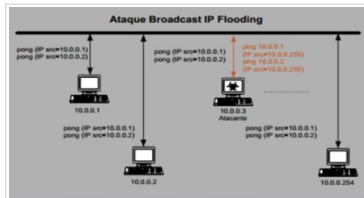
Trabajos Prácticos de Respuesta Múltiple N°8 P2 - CORRECTAS: 1 de 10 - **INSUFICIENTE**

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



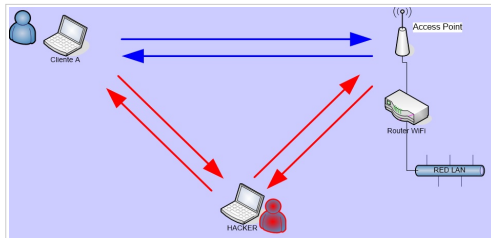
- a) Jamming.
- b) Pharming.
- c) Keylogger.
- ☒ d) Spoofing. **INCORRECTA**
- e) ARP Poisoning.
- f) Ransomware.
- g) Todas las Anteriores son correctas.
- h) Ninguna de las Anteriores es correcta. **CORRECTA**

2) La técnica de Jamming o Flooding o inundación es una técnica que busca generar solicitudes maliciosas a un servicio de internet con la finalidad 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:



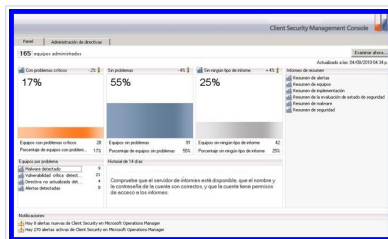
- ☒ a) Fuerza Bruta **INCORRECTA**
- b) Ransomware.
- c) Denegación de Servicio **CORRECTA**
- d) Escaneo de Puertos.
- e) Autenticación.
- f) Ninguna de las Anteriores es correcta.

3) Cuando nos referimos a MAC SPOOFING podemos afirmar que:



- ☒ a) Es un tipo de ataque de robo de identidad. **INCORRECTA**
- b) Es una técnica para clonar la dirección MAC de un dispositivo de red.
- c) Es una Técnica que se utiliza en comunicaciones inalámbricas.
- d) Es una técnica para cambiar la dirección MAC de un dispositivo de red.
- e) Todas las Anteriores son Correctas. **CORRECTA**
- f) Ninguna de las Anteriores es correcta.

4) Un Programa Antivirus dentro de un entorno de red controlado debe cumplir con las siguientes funciones:



- a) La prevención de ejecución de código malicioso y su replicación en memoria.
- b) La protección y bloqueo de Puertos
- ☒ c) Analizar y buscar código malicioso desde archivos hasta comunicaciones (E-mail, tráfico Web, etc.) dentro de nuestro entorno de red, servidores y terminales. **INCORRECTA**
- d) Proteger con sistemas de encriptación la información a ser transportada por la red.
- e) Ambas a y b.
- f) Ambas a y c **CORRECTA**
- g) Ambas a y d.
- h) Ninguna de las Anteriores es correcta.

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

Evaluación

Evaluaciones



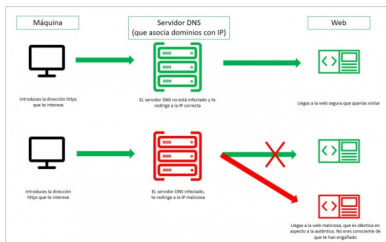
- a) Jamming.
- b) Pharming.
- ☒ c) Keylogger. **INCORRECTA**
- d) Spoofing.
- e) ARP Poisoning.
- f) Ransomware. **CORRECTA**
- g) Todas las Anteriores son correctas.
- h) Ninguna de las Anteriores es correcta.

6) Existe un tipo de peste o alimaña que funciona en su PC, sin su consentimiento o como parte de un consentimiento 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
- ☒ b) Gusano. **INCORRECTA**
- c) Caballo de troya
- d) Virus de sector de Arranque.
- e) Spyware. **CORRECTA**
- f) Ninguna de las Anteriores es correcta.

7) Cuando se realiza una ciberincursión que provoca el "DNS Hijacking" y "DNS Poisoning" que consisten en la publicación ilegítima de resolución de un dominio mediante la modificación de los registros de un servidor DNS, Dicho ataque corresponde a:



- a) Jamming.
- b) Pharming. **CORRECTA**
- ☒ c) Keylogger. **INCORRECTA**
- d) Man in the Middle.
- e) ARP Poisoning.
- f) Ransomware.
- g) Todas las Anteriores son correctas.
- h) Ninguna de las Anteriores es correcta.

8) El Conficker (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 volvia los controladores de dominio lentos. Usaba como modo de propagación las redes y los pendrives. El tipo de virus corresponde a:



- ☒ a) Virus de Macro. **INCORRECTA**
- b) Gusano. **CORRECTA**
- c) Caballo de troya.
- d) Virus de Arranque.
- e) Virus de Script.
- f) Ninguna de las Anteriores es correcta.

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




- a) Keylogger.
- b) Ransomware.
- ☒ c) Phishing. **CORRECTA**
- d) Flooding.
- e) Pharming.

Tecnología de Redes (02-5900)Evaluación

Evaluación

Evaluaciones



a) Keylogger. CORRECTA

b) Ransomware.

c) Jamming.

✖

d) IDS. INCORRECTA

e) Pharming.

f) Ninguna de las Anteriores es correcta.

Observación adicional: TP 8 P2

RESUMEN

Trabajos Prácticos de Respuesta Múltiple N°8 P2

CORRECTAS: 1 de 10

INSUFICIENTE

SALIR

Departamento de Ingeniería e Investigaciones Tecnológicas - Materias Interactivas en Línea - 2022