

# RESUMEN PARA EL EXAMEN DEL 3 TRIMESTRE:

## **HONEY POT:**

Ramsonware – Es un tipo de software malicioso que cifra los archivos o bloquea el acceso al sistema de la computadora mediante técnicas de encriptación. Una vez que los archivos o el sistema están cifrados, el atacante muestra una pantalla de advertencia o envía un mensaje solicitando un rescate, normalmente dinero.

2 tipos de ataques:

1. Dirigidos – Tienen un target concreto y suelen ser realizados por estados o por grupos especializados.
2. No dirigidos – Buscan cualquier sistema que se pueda comprometer en internet.

Honeypot – Es una máquina creada como señuelo o trampa para ser atacada. Normalmente simula ser un objeto valioso y se dejan vulnerabilidades en ella para estudiar y conocer la forma en la que atacan la máquina.

A veces se simulan sistemas de alto interés como Bases de Datos y se dejan vulnerabilidades abiertas para ver es atacada a través de la red.

ALTA INTERACCIÓN – permitimos que ataquen muchos servicios de nuestro HoneyPot

BAJA INTERACCIÓN – permitimos que ataquen pocos servicios exponiendo alguna vulnerabilidad concreta (como dejando abierto un puerto).

Sandbox – son máquinas virtuales muy bien aisladas que se usan para probar malware y ver como actúan en el sistema.

Seguridad por oscuridad – utilizamos un servicio por un puerto poco conocido para que no haya muchos atacantes interesados. No es una medida de seguridad potente pero puede ayudarte a no encontrarte con muchos atacantes al principio.

## **5G :**

### **2-Compartición antenas. Explicación**

En las torres de comunicación, las operadoras móviles comparten el espacio con otras operadoras. De esta forma una torre puede tener antenas de distintas compañías para dar servicio a una misma zona.

### **3-Dividendo digital. Explicación**

El Dividendo Digital fue el proceso de liberación de frecuencias necesario para que la banda 800 MHz quedara disponible en toda Europa. Tras la liberación, la banda de 800 MHz dejó de utilizarse para la transmisión de algunos canales de TDT y se ha asignado a los operadores de telefonía móvil para prestar nuevos servicios de banda ancha de cuarta generación (4G) y ahora de 5G.

### **4-¿qué funciona con 2G, por qué existe aun?**

El 2G sigue existiendo porque tenemos muchos dispositivos que siguen utilizándolo, como por ejemplo los semáforos o algunos datáfonos utilizados en tiendas y restauración. La migración de estos dispositivos a nuevas tecnologías es algo costoso por la cantidad de ellos, por esto, por el momento se seguirá dando soporte a la tecnología 2G.

### **5-Tiempo de concesión banda de 26GHz.**

La banda de 26 GHz tiene un tiempo de concesión de 20 años.

### **6-¿qué significa 4G+?**

La tecnología 4G+ utiliza una técnica que permite a los dispositivos móviles usar múltiples frecuencias de radio 4G para conectarse a la red móvil. Esto permite a los usuarios experimentar velocidades de descarga y carga más rápidas en sus dispositivos móviles.

### **7-Logo 5G en el móvil. ¿Qué significa cuando aparece?**

Significa que tenemos cerca una antena 5G la cual nos llega su frecuencia, no necesariamente significa que estemos experimentando conexión 5G.

### **8-Downlink y uplink**

Downlink es la transmisión de datos desde la antena hasta el dispositivo móvil.

Uplink es la transmisión de datos desde el dispositivo móvil hasta la antena.

### **9-FDD y TDD**

FDD utiliza dos bandas de frecuencia diferentes para la transmisión y recepción de datos, una banda de frecuencia se utiliza para la transmisión de datos (uplink) y otra banda de frecuencia se utiliza para la recepción de datos (downlink).

Por otro lado, TDD utiliza la misma banda de frecuencia para la transmisión y recepción de datos, pero los datos se envían y se reciben en diferentes momentos. La transmisión

y recepción de datos se alternan entre el dispositivo y la antena.

#### 10-Sectorización de antenas

Cuando se requiere dar conexión a una zona concreta, se colocan en la torre de comunicaciones varias antenas direccionales (en vez de colocar una omnidireccional) apuntando a diferentes sectores. De esta forma se garantiza una conexión más estable a un radio concreto. La sectorización de antenas también mejora la calidad de la señal y la cobertura de la red, ya que cada sector se enfoca en una zona específica, reduciendo así la interferencia de señales de otros sectores. Además, también ayuda a reducir el consumo de energía y el costo de la infraestructura, ya que se puede atender a más usuarios con menos antenas y equipos.

#### 11-Beamforming

El beamforming es una técnica basada en la utilización de múltiples antenas para enfocar la señal en una dirección específica, lo que ayuda a mejorar la calidad de la señal y la eficiencia de la transmisión de datos. En las torres de comunicación las antenas 5G están compuestas por muchas antenas más pequeñas que dirigen la señal según dónde se encuentra el dispositivo, de esta forma se asegura que la conexión sea buena para cualquier dispositivo del sector.

#### 12-Mimetizado antenas

El mimetismo de antenas es una técnica de diseño que permite integrar las antenas en objetos dentro de un lugar para hacerlas menos perceptibles y más estéticamente agradables acordes al entorno.



### 13-¿Qué es un modelo de propagación?

Un modelo de propagación es una herramienta matemática utilizada para predecir la propagación de la señal de radio en un medio de transmisión, desde una antena de transmisión a una antena de recepción. Los modelos de propagación se utilizan en el diseño y la planificación de sistemas de comunicaciones inalámbricas y tienen en cuenta factores como la distancia, la frecuencia, la altura y la topografía para predecir la atenuación y la interferencia de la señal.





### 14-Antenas omnidireccionales y sectoriales

La principal diferencia entre las antenas omnidireccionales y sectoriales es la dirección en la que emiten y reciben señales. Las antenas omnidireccionales emiten y reciben señales en todas las direcciones, mientras que las antenas sectoriales emiten y reciben señales en una dirección específica.

### 15-¿Para qué sirve el GPS en antenas?

El GPS en las antenas sirve para que el reloj de todos los dispositivos estén sincronizado y evitar problemas en la comunicación.

	700 MHz	800 MHz	900 MHz	1800 MHz	2100 MHz	2600 MHz	3500 MHz
	5G banda 28	4G banda 20	2G/3G banda 8	2G/4G banda 3	3G banda 1 y 39	4G banda 7 y 38	5G banda 78
Movistar	20 MHz	20 MHz	29,6 MHz	40 MHz	30 MHz FDD 5 MHz TDD	40 MHz nacional 20 MHz autonómico	100 MHz
Vodafone	20 MHz	20 MHz	20 MHz	40 MHz	30 MHz FDD 5 MHz TDD	40 MHz FDD 20 MHz TDD	90 MHz
Orange	20 MHz	20 MHz	20 MHz	40 MHz	30 MHz FDD 5 MHz TDD	40 MHz nacional 40 MHz autonómico	110 MHz
MásMóvil				29,6 MHz	30 MHz FDD 5 MHz TDD	20 MHz TDD (autonómicos)	80 MHz

				
700 MHz (Banda 12) 5G	-	-	-	-
800 MHz (Banda 20) 4G	20 MHz FDD	20 MHz FDD	20 MHz FDD	-
900 MHz (Banda 8) 2G y 3G	30 MHz FDD	20 MHz FDD	20 MHz FDD	-
1.800 MHz (Banda 3) 2G y 4G	40 MHz FDD	40 MHz FDD	40 MHz FDD	30 MHz FDD
2.100 MHz (Banda 1) 3G	30 MHz FDD 5 MHz TDD	30 MHz FDD 5 MHz TDD	30 MHz FDD 5 MHz TDD	30 MHz FDD 5 MHz TDD
2.6 GHz (Banda 7) 4G y 5G	40 MHz FDD 10 MHz FDD Madrid y Melilla	40 MHz FDD 20 MHz TDD	40 MHz FDD 10 MHz TDD 10 MHz FDD España excepto Castilla La Mancha, País Vasco, Asturias, Galicia, Madrid Melilla	10 MHz TDD Madrid, Cataluña, Castilla-La Mancha y Andalucía
3.4/3.8 GHz (Banda 42-43) 5G	90 MHz TDD (40 MHz válidos hasta 2030) (50 MHz válidos hasta 2038)	90 MHz TDD (válidos hasta 2038)	100 MHz TDD (40 MHz válidos hasta 2030) (60 MHz válidos hasta 2038)	80 MHz TDD (válidos hasta 2030)

## NDP:

NDP (Neighbor Discovery Protocol) es un protocolo de la capa de red utilizado en redes de área local (LAN) de Internet Protocol version 6 (IPv6). Su función principal es permitir a los dispositivos en una red IPv6 descubrir y comunicarse entre sí en la misma subred.

El NDP tiene varias funciones importantes:

1. Descubrimiento de vecinos (Neighbor Discovery): Permite a un dispositivo IPv6 descubrir y mantener una lista de los dispositivos vecinos conectados directamente en la misma red. Esto incluye la identificación de direcciones IPv6 y direcciones MAC asociadas a esos vecinos.
2. Autoconfiguración de direcciones IPv6 (Address Autoconfiguration): Permite que los dispositivos IPv6 configuren automáticamente sus direcciones IP sin la necesidad de un servidor DHCP. Los dispositivos pueden generar direcciones IPv6 únicas utilizando información del NDP.
3. Resolución de direcciones (Address Resolution): Permite a los dispositivos IPv6 obtener la dirección MAC de un vecino cuando se conoce su dirección IP. Esto es esencial para la comunicación a nivel de enlace en la red local.

4. Descubrimiento de rutas (Router Discovery): Permite que los dispositivos IPv6 descubran y elijan el mejor enrutador predeterminado en la red local para enviar paquetes fuera de la subred.

En resumen, el NDP es un protocolo utilizado en redes IPv6 que permite el descubrimiento y la comunicación de dispositivos vecinos en la misma red, la autoconfiguración de direcciones IP y la resolución de direcciones para la comunicación a nivel de enlace. Es una parte fundamental para el funcionamiento de redes IPv6 y reemplaza el antiguo protocolo ARP (Address Resolution Protocol) utilizado en IPv4.

## **VLAN:**

VLAN (Virtual Local Area Network o Red de Área Local Virtual, en español). Una VLAN es una técnica que permite dividir una red física en múltiples redes virtuales más pequeñas y aisladas. Cada VLAN actúa como si fuera una red independiente, aunque en realidad comparte el mismo medio físico.

En resumen, una VLAN es una forma de dividir una red física en redes virtuales más pequeñas y aisladas, lo que permite controlar el acceso a los recursos y mejorar la seguridad de la red. En nuestro ejemplo, cada departamento de la oficina estaría en una VLAN separada, lo que limitaría la comunicación y el acceso a recursos solo dentro de cada departamento.

\*\*\*Mira en tus apuntes de VLAN del ejercicio como funciona lo de que los routers cambian los paquetes en la capa de enlace para enviar por VLAN los mensajes\*\*\*

## **VPN:**

Una VPN (Virtual Private Network o Red Privada Virtual) es una tecnología que permite crear una conexión segura y cifrada entre un dispositivo y una red privada a través de una red pública, como Internet. En pocas palabras, una VPN crea un túnel privado y protegido dentro de una red pública.

1. Seguridad: La VPN añade una capa adicional de seguridad al proteger tu conexión y tus datos de posibles ataques o intrusiones. La encriptación de extremo a extremo garantiza que tus datos estén protegidos mientras viajan por la red.
2. Acceso a contenido restringido: Una VPN te permite acceder a contenido en línea que puede estar restringido geográficamente. Al conectarte a un servidor VPN ubicado en otro país, puedes simular estar en esa ubicación y superar las restricciones de contenido.

3. Anonimato: Al enrutar tu tráfico a través de un servidor VPN, tu dirección IP se oculta y se reemplaza por la del servidor VPN. Esto ayuda a preservar tu anonimato en línea y dificulta que terceros rastreen tu actividad.