Universidad Nacional de Ingeniería

Facultad de Ciencias

Escuela Profesional de Ciencia de la Computación

Seguridad Informática

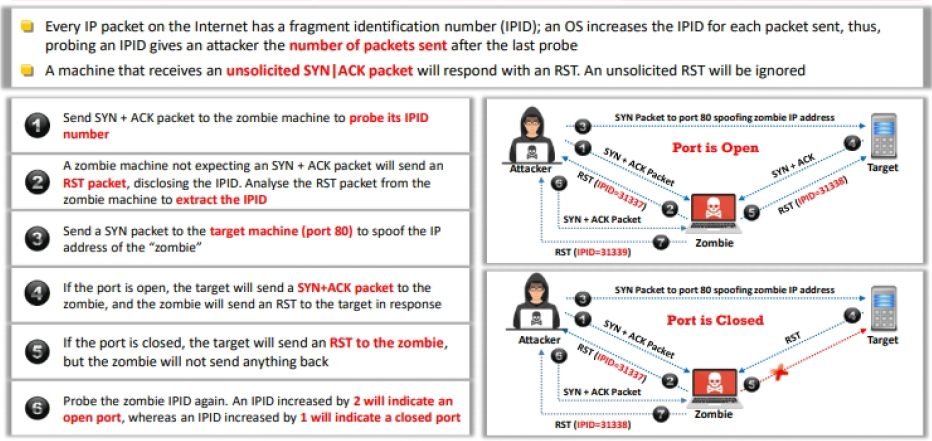
**Práctica de Seguridad Informática**

**SEG Ciclo: 2021-II Fecha:22/10/2021**

**Profesor: Sidney Valer Quispe**

Pregunta 1 (7 puntos)

Implementar en python un escaneo silencioso(idle scanning), es la técnica más sigilosa de realizar un escaneo TCP sobre redes IPv4, ya que oculta la identidad del atacante. Mediante Idle Scanning, el atacante falsifica o suplanta los mensajes enviados desde un tercer host, llamado host inactivo o zombie y utiliza el valor de identificación (**IPID**) en el encabezado IPv4 para ver el resultado del escaneo.



Página 315-318

Pregunta 2 (3 puntos)

Implementar en python la fragmentación de paquetes usando un escaneo SYN/FIN

Página 354-354

Pregunta 3 (5 puntos)

Realizar los laboratorios del capítulo Scaning Networks Pagina 3609 – 3745 y entregar las evidencias

Pregunta 4 (5 puntos)

Teoría: Justificar su respuesta como el siguiente ejemplo: (5 puntos)

1. Los servicios que utilizan un recurso compartido en la red, como los servicios de compartir archivos de red y los servicios de impresión, los recursos de la red pueden ser susceptibles de sufrir uno de los siguientes ataques.
2. Spoofing
3. Null sessions
4. DNS kiting
5. ARP poisoning
6. El administrador de seguridad de una institución menciona que, los usuarios se quejan de la lentitud de la red. Pero en ese momento del día no hay mucha actividad. Para indagar la causa opta por captura paquetes de la red y descubre que se han enviado miles de paquetes ICMP al host. ¿Qué ataque es probable que se esté ejecutando contra su red?
7. Spoofing
8. Man-in-the-middle
9. DNS kiting
10. Denial of service
11. Su red está siendo atacada. Los patrones de tráfico indican que un servicio no autorizado está transmitiendo información a una fuente externa a la red. ¿Qué tipo de ataque se está ejecutando contra usted?

A. Spoofing

B. Man-in-the-middle

C. Replay

D. Denial of service

1. Se detectó un acceso no autorizado en la red. Alguien se ha estado conectando como uno de los técnicos del help desk en horas no laborables. Luego se descubre que un empleado ha recibido un correo electrónico del administrador de la red donde le pide que facilite su contraseña para poder realizar cambios en su perfil. ¿Qué tipos de ataques se han ejecutado?
2. Spoofing
3. Man in the middle
4. Replay
5. Social engineering
6. Cuando se crearon una utilidad para desfragmentar discos duros. Ocultaron un código dentro de la utilidad que se instalará, el sistema infectado borrara el contenido del disco una fecha especificada. ¿Cuál de los siguientes ataques ha sido utilizado en su código?
7. Virus
8. Spoofing
9. Logic bomb
10. Trojan horse
11. Si le asignan la tarea de realizar una auditoría en la red. ¿Cuál es la primera acción que debe realizar?
12. Determinar dónde se almacenarán los archivos de registro.
13. Iniciar inmediatamente a auditar los recursos.
14. Utilizar un escáner de vulnerabilidades para ver qué recursos están mal protegidos.
15. Planificar.
16. La organización sufrió anteriormente un ataque de IP spoofing, Si usted desea hacer algunos cambios en la red para prevenir futuros ataques. ¿Cuál de las siguientes acciones debería realizar?
17. Instalar un software antivirus.
18. Configurar filtros de direcciones IP.
19. Instalar certificados en clientes y servidores.
20. Bloquear todos los puertos del router.
21. El UDP es un protocolo sin conexión que opera en la capa de transporte del modelo OSI y utiliza puertos para gestionar conexiones simultáneas. ¿Cuál de los siguientes términos está también relacionado con UDP?
22. Bits
23. Direccionamiento lógico
24. Reformateo de datos
25. Simplex
26. Una empresa emergente necesita optimizar la entrega de contenidos multimedia de alta definición a sus clientes. Ellos planifican el despliegue de servidores de recursos en numerosos centros de datos de todo el mundo para proporcionar baja latencia, alto rendimiento y alta disponibilidad del contenido alojado. ¿Qué tecnología es probable que se implemente?
27. VPN
28. CDN
29. SDN
30. CCMP
31. ¿Cuál de las siguientes afirmaciones es verdadera sobre el ARP poisoning o MAC spoofing?
32. El MAC spoofing es usado para sobrecargar la memoria de un switch.
33. El ARP poisoning se utiliza para falsificar la dirección física de un sistema para suplantar la de otro dispositivo autorizado.
34. El MAC spoofing se basa en comunicaciones ICMP para atravesar los routers.
35. El ARP poisoning puede usar respuestas no solicitadas o gratuitas.