Trabajo Práctico N° 4

Conceptos de seguridad

Fecha Límite de Entrega: 24 de mayo a las 23:55
Profesor: Dr. Javier Echaiz
Auxiliar: Ing. Fernando Pap

Condiciones de Aprobación:

En líneas generales el trabajo debe dar evidencia del desarrollo realizado. En casos puntuales en los que sea conveniente, incluir un archivo `readme.txt` con notas correspondientes. Entregas individuales subiendo contenido al directorio `ARS2018/Entregas/[nombre]` del Google Drive y enviando aviso al email fernandopap@gmail.com o al grupo de whatsapp. Se recomienda utilizar github/ Bitbucket/etc.
El trabajo debe ser entregado completo. Pasada la fecha límite de entrega se descontará un punto por cada día transcurrido.

Enunciados

1. Explique y relacione los conceptos de:
    - Vulnerabilidad
    - Amenaza
    - Incidente

2. Explique el concepto de seguridad "en capas".

3. Investigue/analice los riesgos introducidos en una organización por uso de redes sociales y mensajería instantánea.

4. Términos relacionados: Busque la definición correspondiente a cada uno de los siguientes términos. Exploit - Malware - Buffer Overflow - Troyano - Shellcode - Ransomware - Fuerza bruta - DOS - DDOS - Bot - Botnet - Flooding - SPAM - Cracking - 0day - MITM - Hoax - Rootkit - Backdoor - Phishing - Bug - Pharming - Ingenieria Social - Sniffing - Spoofing - Scanning - Script Kiddie.

5. ¿Qué problemas de seguridad puede provocar un ataque de sniffing sobre tráfico SMTP, POP o HTTP? ¿Desde qué red/redes tiene sentido dicho ataque?

6. Una dirección MAC: ¿Se puede falsificar? ¿Desde qué red tiene sentido dicho ataque? ¿Con qué objetivo alguien malintencionado lo haría?

7. Analice cómo funciona el protocolo ARP. ¿Qué ataque podría realizar alguien malintencionado usando este protocolo? ¿Desde qué red tendría sentido dicho ataque?

9. Una dirección IP: ¿Se puede falsificar? ¿Desde qué red tendría sentido dicho ataque? ¿Con qué objetivo alguien malintencionado lo haría?

10. Analice cómo funciona el protocolo ICMP. ¿Qué ataque puede realizar alguien malintencionado usando este protocolo? ¿Desde qué red tendría sentido dicho ataque?

11. Analice cómo funciona el protocolo DNS. ¿Qué ataque podría realizar alguien malintencionado usando este protocolo? ¿Desde qué red tendría sentido dicho ataque? ¿Qué mejoras se han propuesto sobre DNS?

12. OWASP:
    a) Describa brevemente el objetivo de la organización.
    b) ¿Cuáles fueron los tres riesgos más críticos de seguridad en aplicaciones web en el año 2017?
    c) ¿Qué información puede encontrar acerca de Ransomware?