Técnicas de Envenenamiento de redes de datos

Omar Gonzalez
Soluciones Seguras

SOLUCIONES SEGURAS

Agenda

- Spoofing
- DNS Hijaking
- Phishing
- Mail Spoofing

SOLUCIONES SEGURAS

Agenda

- Spoofing
  - ¿Que significa Spoof?
    - Falsificar información haciéndola ver real.

- Spoofing - tipos
  - Ip Address Spoofing
  - MAC Spoofing
  - URL Soofing
  - Caller ID Spoofing
  - Protocol Spoofing
  - SMS Spoofing

- DNS Hijaking
  - Secuestro de DNS
  - Whitehat
    - Cambiar el ip de facebook a una ip inválida.
    - Configuración de una resolución de nombre interno
  - Blackhat
    - Cambiar el IP de un nombre para dirigir a otro lugar
    - Mandar a un sitio donde bajan malwares para instalar en las maquinas
    - Defacement

- DNS Hijaking
  - Como protege o evitar
    - DMZ
    - Control de Acceso
    - Control de Cambios estrictos
    - Registar-Lock

- Phishing
  - Hacerse pasar por una entidad confiable para obtener información
  - Tipos
    - Link Manipulation
    - Phone Phishing
    - Tabnabbing
  - Como evitarlo
    - Legitimidad de los sigtios WEB (Autoridad Certificadora)
    - Filtros SPAM que conozcan de Phishing para su detección
    - Aumento de la forma de autenticación de usuarios, imágenes preguntas personales.
    - Contribuir al reportes de un atentado al momento de enfrentar uno

Phishing ejemplo:

From: ASOCIACION BANCARIA DE PANAMA [mailto:avg@asociacionbancariapanama.com]
Sent: Sunday, March 18, 2012 4:44 AM
To: [redacted]
Subject: LIBERATE DE VIRUS AQUI !
Importance: High

La Asociación Bancaria de Panamá en coordinación con la Superintendencia de Bancos de Panamá, La Superintendencia de Seguros y Reaseguros, La Comisión nacional de Valores, El Ministerio Publico, y una prestigiosa firma de Antivirus, han firmado un acuerdo que beneficiará a los clientes de todos los bancos afiliados, brindándole una mayor seguridad, ante lo cual pone a disposición una aplicación que protegerá su equipo de cómputo, de cualquier ataque de piratas informáticos que pretendan obtener sus claves bancarias e información personal poniendo en riesgo su seguridad, y se lo trae en forma gratuita únicamente por el periodo de 48 horas, a partir de recibido haber este mail.

Recomendamos a todos los usuarios a descargar esta aplicación que le dará la seguridad necesaria y evitará futuras perdidas, además comunicamos que en los próximos días, para mantener sus cuentas activas se le pedirá como requisito tener este programa instalado en sus equipos de cómputo, gracias.

SOLUCIONES SEGURAS

- Mail Spoofing
  - Falcificar un correo para hacerlo ver real.
  - Aparentar ser de un dominio diferente es muy fácil
    - Mandar un e-mail de mickey@disney.com es muy facil
  - Varias razones para utilizar este tipo de ataque:
    - La persona que envía correos SPAM no se quiere meter en problemas
    - El tipo de correo que esta enviando viola alguna ley.
    - El correo contiene algún virus o troyano el cual sería abierto si aparenta ser de otra persona
    - Ataque de ingeniería social
    - Causa problemas enviando un correo con información relevante, haciéndose pasar por otra persona.

- Mail Spoofing
  - E-mail Spoof Protection podría bloquear usuarios externos
    - Esto no permite que el antispam reciba correos desde dominios que protege.
    - No permitiría que un usuario desde su casa envíe un correo originándose de su dominio
  - SPF (Sender Spoof Protection) podría causar pérdida de muchos correos
    - SPF requiere de una entrada especial en los DNS.
    - Requiere también una entrada PTR del servidor.
    - Pocos dominios tienen bien configurado el SPF

Gracias

SOLUCIONES SEGURAS