Seguridad en Sistemas Informáticos

Ingeniería social

Mikel Izal Azcárate
(mikel.izal@unavarra.es)

Indice

- Ingeniería social
- Técnicas básicas
- Combatiendo la ingeniería social

El eslabón más débil

- "You could spend a fortune purchasing technology and services...and your network infrastructure could still remain vulnerable to old-fashioned manipulation."

  -Kevin Mitnick

- The easiest way to break into any computer system is to use a valid username and password and the easiest way to get that information is to ask someone for it.

- Yes it is people who are the weakest link in any security system and Social Engineering Exploits that ---

Ingeniería social

- Métodos psicológicos
- Explotar la tendencia a confiar en las personas
- Más fácil que el hacking técnico
- Y más difícil de detectar y rastrear

- Ingenieros sociales
  - Actores mas que hackers
  - Observar a las personas e interpretar como se sienten
  - Manipular los sentimientos con lo que dicen
  - Hacer que la víctima quiera darte la información

4 aproximaciones básicas

- Descuido
- Comodidad/tranquilidad (confort zone)
- Solidaridad y ayuda
- Miedo

Explotando el descuido

- La víctima es descuidada
  - No se preocupa por poner las contramedidas y protocolos adecuados
- Lo que hay en los alrededores
- Util para reconocimiento...
- Ejemplos
  - Mucha información en la basura (parece de poca importancia pero permite hacerse una idea interna de la organización)
  - Contraseñas apuntadas dejadas por ahi
  - Recolección de contraseñas (uso de la misma contraseña en diferentes cuentas)

Explotando confort zone

- En un entorno confortable
  - no pensamos en posibles amenazas
  - tendencia a pensar que todo está bien/es normal
- Hacerse pasar por compañeros, jefes, mantenimiento, cualquiera de la empresa al que no conozca pero tiene automáticamente la confianza
- Shoulder surfing (observar lo que escriben) o utilizar terminales dejados sin bloquear
- Entrada con la autorización de otro (esperar en la zona de fumadores...)
- Troyanos sociales (el CD, USB abandonado con información curiosa..)

Explotando la solidaridad

- Nos sentimos bien ayudando al projimo
- Simplemente llamar pidiendo ayuda (para conocer procedimientos internos)
- Conseguir un nombre de usuario y pedir que se resetee la contraseña
- Piggybacking (entrar usando la autorización de otro... pasar cerca de otro, fingir que has perdido la llave/tarjeta, llevar una caja en las manos y no poder abrir la puerta...)

Explotando el miedo

- Mas agresivo. En un estado de miedo/ansiedad no nos preocupamos por otras amenazas
- Petición con urgencia
  - parece que corre prisa y pasara algo malo si no...
  - tu cuenta bancaria sera desactivada si no insertas aqui la contraseña,
  - necesito la cuenta para enviar este proyecto ya, si no la culpa sera tuya...
  - especialmente si parece que la responsabilidad sera compartida
- Petición con autoridad
  - le vas a pedir verificación a tu jefe si te dice que le borres la contraseña o no sigas el procedimiento?

Otros...

- Ingeniería social a la inversa

  Lograr que la que la víctima intente conseguir algo del ingeniero social. Puedes preguntarle lo que necesites para resolver su problema (que puede ser ficticio)
- Ejemplos:
  - Provocar una avería de red para que la victima te pida resolverla. Como ha llamado el se fiara si le pides su nombre de usuario/ contraseña
  - Timos clásicos en los que la víctima intenta timar a alguien pero debe un poco de dinero para luego conseguir mas

Técnicas de ingeniería social

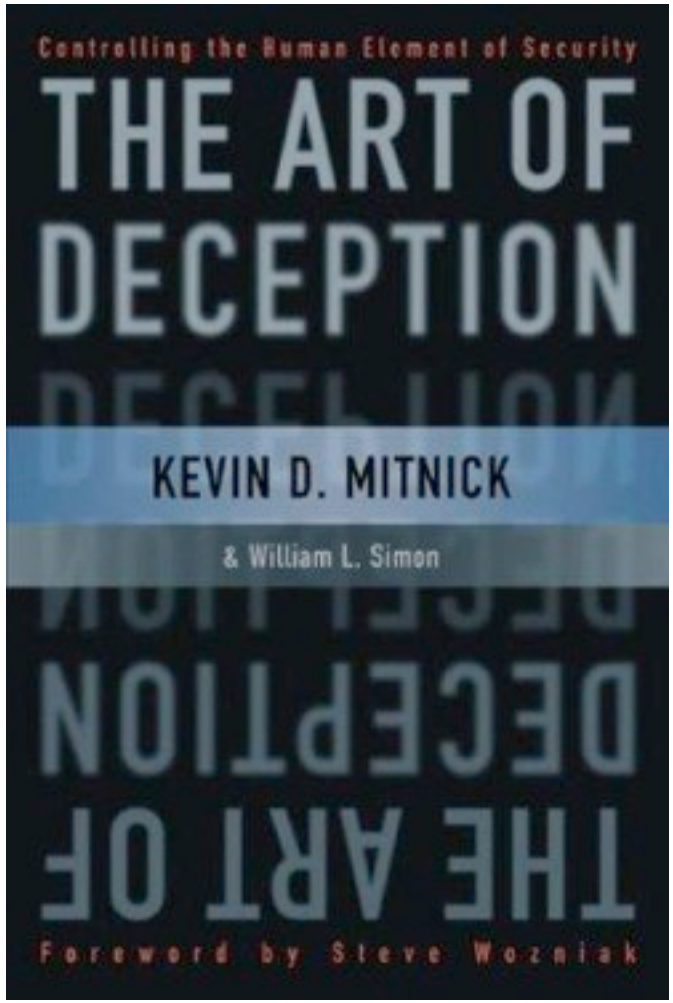
- Pretexting
- Phising
- Spear phising
- IVR/Phone phising
- Trojan horses
- Shoulder surfing
- Dumpster diving
- Road apples
- Quid pro quo

Contramedidas

- No se puede proteger con tecnología
- Educación a los usuarios y entrenamiento
  - No compartir passwords, no apuntarlas
  - Reconocer phising y no fiarse de los enlaces o telefonos en mails
  - Bloquear la pantalla del ordenador con contraseña
  - No dejar a extraños usar tarjetas/llaves, no dejar visitantes sin compañia...
  - No dar información confidencial por telefono...
- Identificar áreas de riesgo
  - Medidas específicas por área
- Política de seguridad bien diseñada, que se aplique y que sea verificada
  - Reconocer ataques
  - Tener instrucciónes de que hacer (que responder a una peticion confidencial, a quien informar si se produce)
  - Monitorizar y vigilar, hacer auditorias...

Para leer sobre estos temas...

- The art of deception
  Kevin D. Mitnick



Conclusiones

- La ingeniería social es una amenaza hoy en día
- Se puede combinar con las técnicas anteriores de hacking para completarlas
  - Convencer a alguien para que me de un usuario y pass facil y escalar privilegios desde ahi
  - Enumerar servicios y otra información con nmap para que luego el escenario que explique por telefono resulte totalmente creible
  - Hacer un backdoor individualizado que salga de un firewall y me de información e instalarlo mediante la técnica de dejar un USB olvidado dentro de una empresa
  - ...
- Hay que estar preparado con reglas para actuar
- Habéis recibido algún ataque de este tipo?