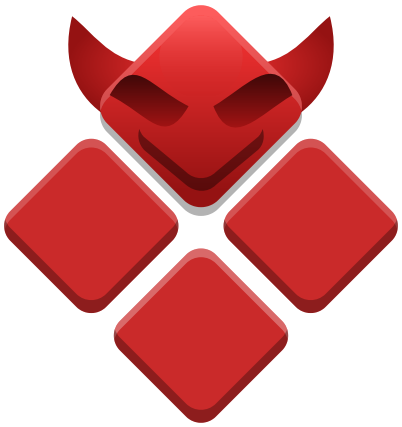
Evil-Winrm



version: 3.7 arch: all

Evil-Winrm Homepage | Package Tracker | Source Code Repository

Edit This Page

Metapackages

default everything large

Packages & Binaries

evil-winrm

evil-winrm

Learn more with OffSec

Pen-200 Soc-200

Packages and Binaries:

evil-winrm

This package contains the ultimate WinRM shell for hacking/pentesting.

WinRM (Windows Remote Management) is the Microsoft implementation of WS-Management Protocol. A standard SOAP based protocol that allows hardware and operating systems from different vendors to interoperate. Microsoft included it in their Operating Systems in order to make life easier to system administrators.

This program can be used on any Microsoft Windows Servers with this feature enabled (usually at port 5985), of course only if you have credentials and permissions to use it. So it could be used in a post-exploitation hacking/pentesting phase. The purpose of this program is to provide nice and easy-to-use features for hacking. It can be used with legitimate purposes by system administrators as well but the most of its features are focused on hacking/pentesting stuff.

It is using PSRP (Powershell Remoting Protocol) for initializing runspace pools as well as creating and processing pipelines.

Installed size: 146 KB
How to install: sudo apt install evil-winrm

Dependencies:

- ruby
- ruby-fileutils
- ruby-logger
- ruby-stringio
- ruby-winrm
- ruby-winrm-fs

evil-winrm

```
root@kali:~# evil-winrm -h

Evil-WinRM shell v3.7

Usage: evil-winrm -i IP -u USER [-s SCRIPTS_PATH] [-e EXES_PATH] [-P PORT
    -S, --ssl                        Enable ssl
    -a, --user-agent USERAGENT       Specify connection user-agent (defau
    -c, --pub-key PUBLIC_KEY_PATH    Local path to public key certificate
    -k, --priv-key PRIVATE_KEY_PATH  Local path to private key certificat
    -r, --realm DOMAIN               Kerberos auth, it has to be set also
    -s, --scripts PS_SCRIPTS_PATH    Powershell scripts local path
        --spn SPN_PREFIX             SPN prefix for Kerberos auth (defaul
```

```
    -e, --executables EXES_PATH      C# executables local path
    -i, --ip IP                      Remote host IP or hostname. FQDN fo
    -U, --url URL                    Remote url endpoint (default /wsman
    -u, --user USER                  Username (required if not using ker
    -p, --password PASS              Password
    -H, --hash HASH                  NTHash
    -P, --port PORT                  Remote host port (default 5985)
    -V, --version                    Show version
    -n, --no-colors                  Disable colors
    -N, --no-rpath-completion        Disable remote path completion
    -l, --log                        Log the WinRM session
    -h, --help                       Display this help message
```

Learn more with

Want to learn more about evil-winrm? get access to in-depth training and hands-on labs:

PEN-200: 17.1.4. Windows Privilege Escalation: Information Goldmine PowerShell
SOC-200: 5. Windows Client-Side Attacks

PEN-200 course

SOC-200 course

Updated on: 2025-Nov-18

Edit this page

LIGHT DARK

Links

Home

Download / Get Kali

Blog

OS Documentation

Tool Documentation

System Status

Archived Releases

Partnerships

Platforms

ARM (SBC)

NetHunter (Mobile)

Amazon AWS

Docker

Linode

Microsoft Azure

Microsoft Store (WSL)

Vagrant

Development

Bug Tracker

Continuous Integration

Community

Discord

Support Forum

Network Mirror

Package Tracker

GitLab

PeerTube

Follow Us

Bluesky

Facebook

Instagram

Mastodon

Substack

X

Newsletter

RSS

Policies

Cookie Policy

Privacy Policy

Trademark Policy

OffSec™

Kali Linux is part of OffSec's Community Projects
Learn more about OffSec's free, open-source penetration testing tools for cybersecurity professionals