

Rapid7

By Rapid7

Archived: 2026-04-05 20:49:31 UTC

module

Service Persistence

Disclosed	Created
Jan 1, 1983	May 30, 2018

Disclosed

Jan 1, 1983

Created

May 30, 2018

Description

This module will create a service on the box, and mark it for auto-restart.

We need enough access to write service files and potentially restart services

Targets:

System V:

CentOS

Debian

Kali 2.0

Ubuntu

Upstart:

CentOS 6

Fedora >= 9,

Ubuntu >= 9.10,

systemd:

CentOS 7

Debian >= 7,

Fedora >= 15

Ubuntu >= 15.04

Note: System V won't restart the service if it dies, only an init change (reboot etc) will restart it.

Authors

h00die mike@shorebreaksecurity.com

Cale Black

Platform

Linux,Unix

Architectures

cmd

Module Options

To display the available options, load the module within the Metasploit console and run the commands 'show options' or 'show advanced':

```
msf > use exploit/linux/local/service_persistence
msf exploit(service_persistence) > show targets
...targets...
msf exploit(service_persistence) > set TARGET < target-id >
msf exploit(service_persistence) > show options
...show and set options...
msf exploit(service_persistence) > exploit
```

NEW

Explore Exposure Command

Confidently identify and prioritize exposures from endpoint to cloud with full attack surface visibility and threat-aware risk context.

Source: https://www.rapid7.com/db/modules/exploit/linux/local/service_persistence