GitHub - sensepost/ruler: A tool to abuse Exchange services

By staaldraad

Archived: 2026-04-05 14:08:16 UTC

Introduction

Ruler is a tool that allows you to interact with Exchange servers remotely, through either the MAPI/HTTP or RPC/HTTP protocol. The main aim is abuse the client-side Outlook features and gain a shell remotely.

The full low-down on how Ruler was implemented and some background regarding MAPI can be found in our blog posts:

- Ruler release
- Pass the Hash with Ruler
- Outlook forms and shells
- Outlook Home Page – Another Ruler Vector

For a demo of it in action: Ruler on YouTube

What does it do?

Ruler has multiple functions and more are planned. These include

- Enumerate valid users
- Create new malicious mail rules
- Dump the Global Address List (GAL)
- VBScript execution through forms
- VBScript execution through the Outlook Home Page

Ruler attempts to be semi-smart when it comes to interacting with Exchange and uses the Autodiscover service (just as your Outlook client would) to discover the relevant information.

Getting Started

Compiled binaries for Linux, OSX and Windows are available. Find these in Releases information about setting up Ruler from source is found in the getting-started guide.

Usage

Ruler has multiple functions, these have their own documentation that can be found in the wiki:

- BruteForce -- discover valid user accounts
- Rules -- perform the traditional, rule based attack

- Forms -- execute VBScript through forms
- Homepage -- use the Outlook 'home page' for shell and persistence
- GAL -- grab the Global Address List

Attacking Exchange

The library included with Ruler allows for the creation of custom message using MAPI. This along with the Exchange documentation is a great starting point for new research. For an example of using this library in another project, see SensePost Liniaal.

License