
















 master ▾

Go to file

 Code ▾

🕒

 autodiscover		
 forms		
 http-ntlm		
 mapi		
 rpc-http		
 templates		
 utils		
 webdav		
 .gitignore		
 LICENSE		
 Makefile		
 README.md		
 go.mod		
 go.sum		

About


A tool to abuse Exchange services


exchange


mapi


pentesting


shells


 Readme


 View license

 Activity

 Custom properties


 2.2k stars

 99 watching

 357 forks

Report repository

Releases 18

 **Dependency Update** Latest

on Feb 19, 2021

[+ 17 releases](#)

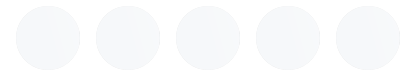
Packages

No packages published

Contributors 5

📄 ruler.go

📖 README License



## Languages

● Go 99.8% ● Makefile 0.2%

# 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

License CC BY-NC-SA 4.0

Ruler is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License (<http://creativecommons.org/licenses/by-nc-sa/4.0/>)

Permissions beyond the scope of this license may be available

at <http://sensepost.com/contact/>

[Terms](#) [Privacy](#) [Security](#) [Status](#) [Docs](#) [Contact](#) [Manage cookies](#) [Do not share my personal information](#)



© 2024 GitHub, Inc.