GitHub - sensepost/notruler: The opposite of Ruler, provides blue teams with the ability to detect Ruler usage against Exchange.

By Etienne Stalmans

Archived: 2026-04-06 01:54:04 UTC

Introduction

NotRuler is the opposite of Ruler. The tool aims to make life a little easier for Exchange Admins by allowing for the detection of both client-side rules and VBScript enabled forms. At a miminum this should allow for the detection of all attacks created through Ruler.

NotRuler allows you to interact with Exchange servers remotely, through either the MAPI/HTTP or RPC/HTTP protocol.

What does it do?

NotRuler can query one or more Exchange mailboxes and detects client-side Outlook rules and VBScript enabled forms.

- Allows Exchange Admins to check for compromise
- Check your own account for compromise
- Extract stager address for Malicious rules
- Extract VBScript used in forms
- Check for 'homepage' and extract URL

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].

NotRuler has two modes of operation:

- Rules -- check for client-side rules
- Forms -- check for VBScript enabled forms
- Homepage -- check for a custom homepage

Rules

The current version of NotRuler can check either a single or multiple mailboxes. These are supplied in the program arguments.

To check multiple mailboxes, create a file with one account per line:

```
 john.ford@testdomain.com
henry.hammond@testdomain.com
james.smith@testdomain.com
cindy.shell@testdomain.com
```

Using the Exchange Admin account, you should be able to log into any mailbox on the Exchange server:

```
./notruler --username exchangeadmin --mailboxes /path/to/mailbox.list rules
```

You can also check your own account by using `--self`

```
./notruler --username john.ford@testdomain.com --mailbox john.ford@testdomain.com --self rules
```

Sample output:

```
 [+] Checking [john.ford@testdomain.com]
[+] Found 5 rules
[WARNING] Found client-side rule: [01000000d97851c4:pewpew3] Application: [\\myhost.somewhere.darkside.com\dav\r
[WARNING] Found client-side rule: [01000000d97851b9:pewpew] Application: [\\myhost.somewhere.darkside.com\dav\ba
[+] Checking [cindy.shell@testdomain.com]
[+] No Rules Found
[+] Checking [henry.hammond@testdomain.com]
[+] No Rules Found
[+] Checking [james.smith@testdomain.com]
[+] No Rules Found
```

Forms

Same as with Rules, you need to either have a list of mailboxes or a single mailbox to check. Simply swap "rules" for "forms":

Using the Exchange Admin account, you should be able to log into any mailbox on the Exchange server:

```
./notruler --username exchangeadmin --mailboxes /path/to/mailbox.list forms
```

You can also check your own account by using `--self`

```
./notruler --username john.ford@testdomain.com --mailbox john.ford@testdomain.com --self forms
```

Sample output:

```
 [+] Checking [john.ford@testdomain.com]
[WARNING] Found form with VBScript! [IPM.Note.badform]
    Function P()
CreateObject("Wscript.Shell").Run "powershell.exe -NoP -sta -NonI -W Hidden -Enc WwBTAFkAUwB0AEUAbQAuAE4AZQBUAC4

[+] Checking [cindy.shell@testdomain.com]
[+] Checking [henry.hammond@testdomain.com]
[+] Checking [james.smith@testdomain.com]
```

Homepage

And the same again, you need to either have a list of mailboxes or a single mailbox to check.

Using the Exchange Admin account, you should be able to log into any mailbox on the Exchange server:

```
./notruler --username exchangeadmin --mailboxes /path/to/mailbox.list homepage
```

You can also check your own account by using `--self`

```
./notruler --username john.ford@testdomain.com --mailbox john.ford@testdomain.com --self homepage
```

Sample output:

```
 [+] Checking [john.ford@testdomain.com]
[WARNING] Found endpoint: http://attack.attackpew.com/rce.html
[+] Webview is set as ENABLED
[+] Checking [cindy.shell@testdomain.com]
[+] Checking [henry.hammond@testdomain.com]
[+] Checking [james.smith@testdomain.com]
```

IOCs

I've added a list of IOC's here: iocs.md

Feel free to submit Issues/PRs with further IOCs!

License

Source: https://github.com/sensepost/notruler