OWNING O365 THROUGH BETTER BRUTE-FORCING

May 14, 2019

By TrustedSec in Office 365 Security Assessment, Penetration Testing, Security Testing & Analysis

SEARCH THE BLOG

SEARCH

SEARCH BY AUTHOR

All Authors

BROWSE BY DATE

BROWSE BY CATEGORY

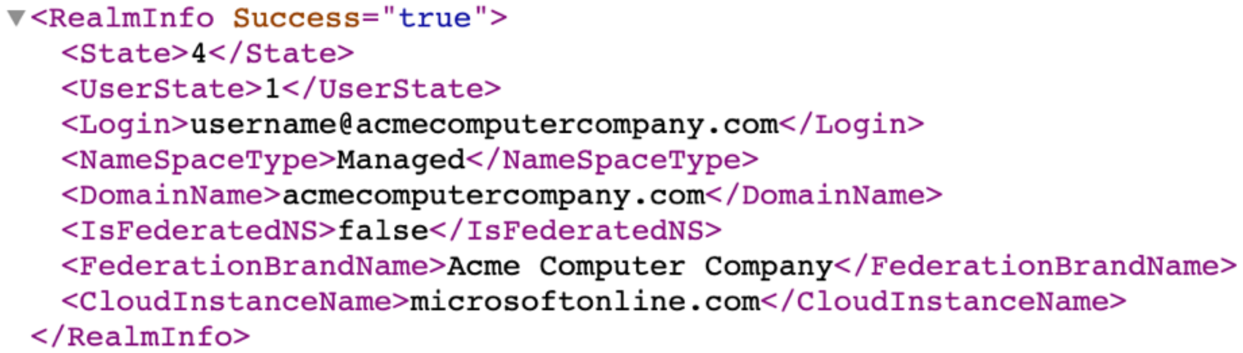
All Categories ▼

TL;DR:

Office 365 (O365) has become a trend in organizations. More and more, administrators are offloading their mail to The Cloud™. No longer are admins shackled to their Exchange servers, executing patch after patch in hopes of staying ahead of the evil hackers! No, Microsoft will take care of that now. Sleep soundly, Exchange server admins, your mail servers are in good hands. While it is increasingly common for organizations to swap their on-premises Exchange servers for O365, they still face the same threats. Like the Exchange servers that came before it, O365 also has a user-enumeration flaw. And, since Microsoft does not consider user-enumeration to be a bug, O365 is as great of a target for brute-force attacks as any Exchange server ever was. For this reason, O365 is one of the first things I look for in an engagement, because it will often result in credentials.

How can we tell if an organization uses O365? We can check with a single URL:

https://login.microsoftonline.com/getuserrealm.srf?login=username@acmecomputercompany.com&xml=1



```
▼<RealmInfo Success="true">
    <State>4</State>
    <UserState>1</UserState>
    <Login>username@acmecomputercompany.com</Login>
    <NameSpaceType>Managed</NameSpaceType>
    <DomainName>acmecomputercompany.com</DomainName>
    <IsFederatedNS>false</IsFederatedNS>
    <FederationBrandName>Acme Computer Company</FederationBrandName>
    <CloudInstanceName>microsoftonline.com</CloudInstanceName>
  </RealmInfo>
```

Figure 1 – Testing for O365

If the ‘NameSpaceType’ indicates ‘Managed,’ then O365 is in use. Other values are ‘Federated,’ for Federated Active Directory, and ‘Unknown,’ if no record exists.

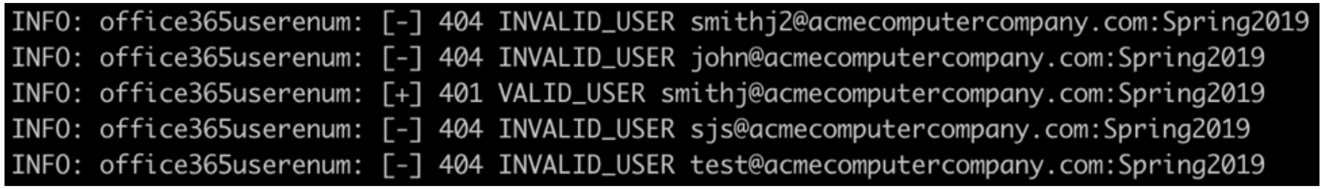
It’s Not a Bug, It’s a Feature!

Microsoft doesn’t consider user enumeration to be a security problem. It has demonstrated this by refusing to fix a well-known user enumeration timing bug in Outlook Web Access (OWA) for years (http://h.foofus.net/?p=784). It has likewise refused to fix a similar issue in Microsoft Lync/Skype for Business (https://github.com/nyxgeek/lyncsmash). In fact, the Microsoft security reporting page states quite clearly that it does not consider user enumeration to be a problem —it’s not a bug, it’s a feature.

exist.

Response Code	Description
200	Successful login (good user/password)
401	Valid Username, bad password
403	Valid Username, good password, 2FA required
404	Invalid Username

A tool called Office365UserEnum (https://bitbucket.org/grimhacker/office365userenum) was released a couple years organizations might not detect the attack.



```
INFO: office365userenum: [-] 404 INVALID_USER smithj2@acmecomputercompany.com:Spring2019
INFO: office365userenum: [-] 404 INVALID_USER john@acmecomputercompany.com:Spring2019
INFO: office365userenum: [+] 401 VALID_USER smithj@acmecomputercompany.com:Spring2019
INFO: office365userenum: [-] 404 INVALID_USER sjs@acmecomputercompany.com:Spring2019
INFO: office365userenum: [-] 404 INVALID_USER test@acmecomputercompany.com:Spring2019
```

Figure 2 O365 User Enumeration

When parsing the results of this tool for successful logins, I like to use grep -v to remove the 404 and 401 responses. This will leave you with a short list of the 200s, as well as any valid 2FA (403), and any responses that generated an error (400 or 500). In my experience, it is worth double-checking and manually testing any returned 400 codes, as this could indicate a successful login that failed for some other reason.

Better Brute-Forcing

The O365 brute-force requires a list of email addresses to attack. I would recommend searching password dumps (e.g., LinkedIn or Adobe breach) for email addresses. Some sites like hunter.io specialize in providing email addresses for different organizations. A fairly reliable method is to generate your own by using a list of statistically-likely-usernames (https://github.com/insidetrust/statistically-likely-usernames) and turning them into email addresses. This is easy to do in Linux:

(Spring2019) and we're on our way.

If we're lucky, we will get a set of credentials off the bat. If we fail, it's probably because we haven't done a good enough job of user enumeration. Check the size of your target organization on LinkedIn or Wikipedia. Know how many users you should expect to find. If you have an organization of 50,000 but only have 500 valid accounts, you've got some work to do.

If you're banging your head against the wall trying to find new names to try, revisit your valid users list. Take any last names and use a one-liner to combine first names with your already-discovered last names.

```
while read firstname; do
while read lastname; do echo "$firstname.$lastname@domain.com"; don
< lastnames.txt ; done < firstnames.txt
```

Example Output:

adam.anderson@domain.com

adam.rogers@domain.com

bob.rogers@domain.com

bob.smith@domain.com

carly.anderson@domain.com

carly.rogers@domain.com

carly.smith@domain.com

When all else has failed, I've had luck using a Google dork with LinkedIn to discover new names for enumeration.

```
site:linkedin.com
intext:<company name>
```

Remember that a company may have multiple username formats in play. If you're failing to find more usernames with a given format, try other formats. The statistically-likely-usernames list has a top-formats.txt that works well (https://github.com/insidetrust/statistically-likely-usernames/blob/master/top-formats.txt).

the users_tried.txt file, and we output the resulting list to a 'new_users_untried.txt' file.

```
comm -13 users_tried.txt new_users_generated.txt > new_users_untrie
```

Obviously, the bigger the organization, the better. Unless the organization has a crazy-awesome password policy, you will get an account.

In my experience, most brute-force failures stem from a failure to enumerate enough users. SOMEBODY has a bad password. One password is all we need.

Classic Passwords Still Work

As long as a 90-day password change policy exists, so will seasonal and month-related passwords. This style of password should be your go-to for initial attempts:

Spring2019

Spring19

Spring19!

Password1

P@ssw0rd

Password123

Company1

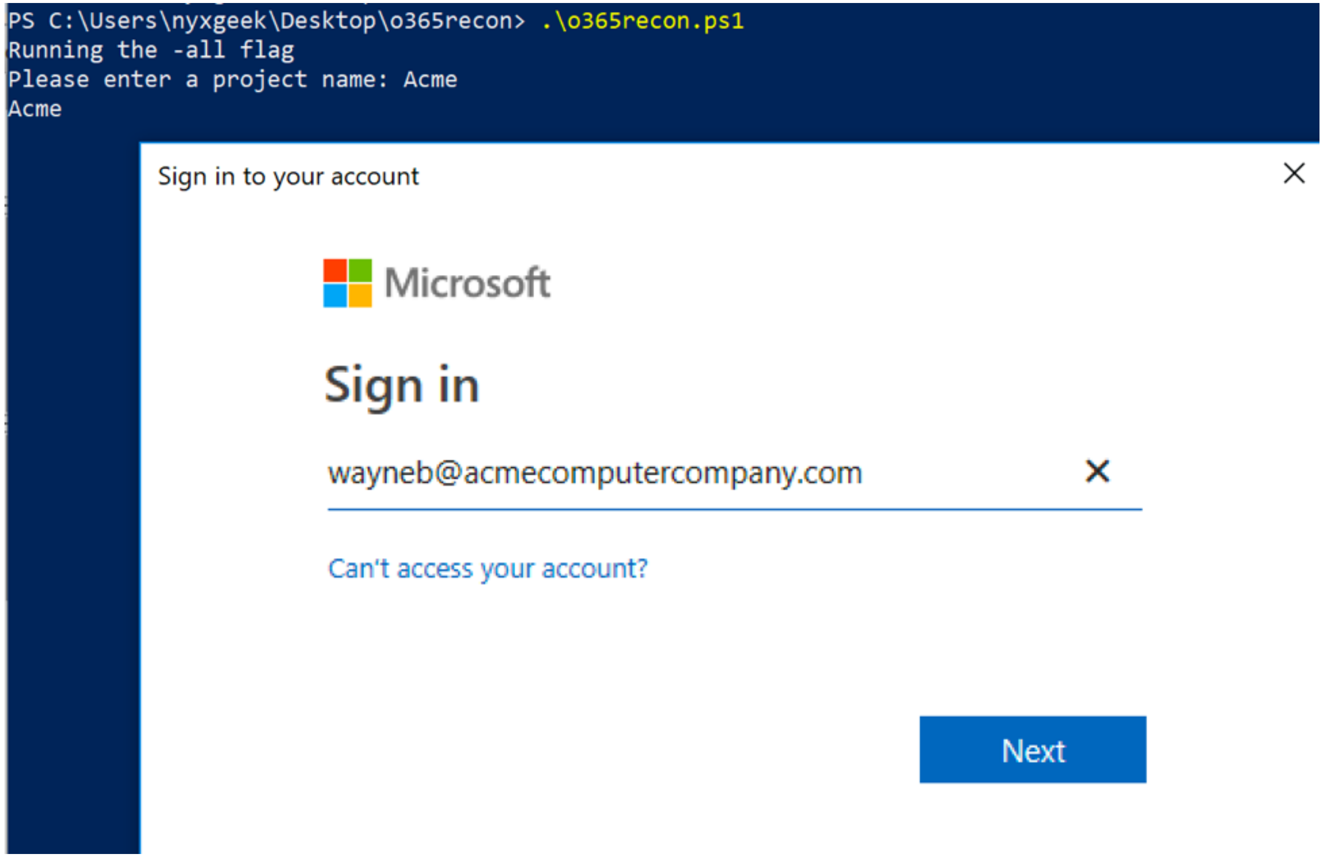
Company123

These are not uncommon. You'd be surprised. If you're not finding any users with these passwords, I would recommend going back to user enumeration and finding more users.

NOTE: By default, O365 has a lockout policy of 10 tries, and it will lock out an account for one (1) minute. However, if it is synced with on-premises, this means that the actual lockout could be much lower. Additionally, Azure AD allows for custom lockout settings (https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-password-smart-lockout). Keep this in mind while testing.

We Got One! (Now Let's Get More)

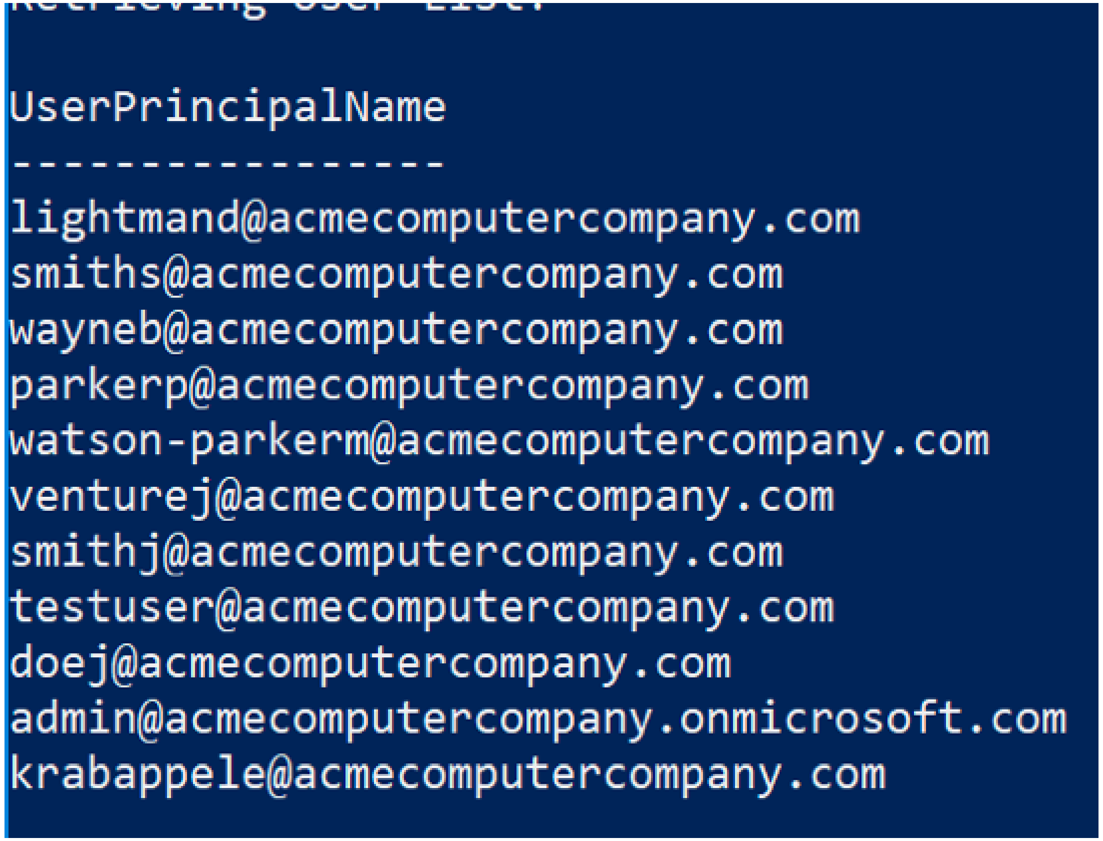
other information—basically, LDAP queries via O365 and PowerShell. I've compiled the various PowerShell commands into a script: o365recon (https://github.com/nyxgeek/o365recon).



```
PS C:\Users\nyxgeek\Desktop\o365recon> .\o365recon.ps1
Running the -all flag
Please enter a project name: Acme
Acme
```

wayneb@acmecomputercompany.com

Figure 3 – Connecting to O365 with o365recon

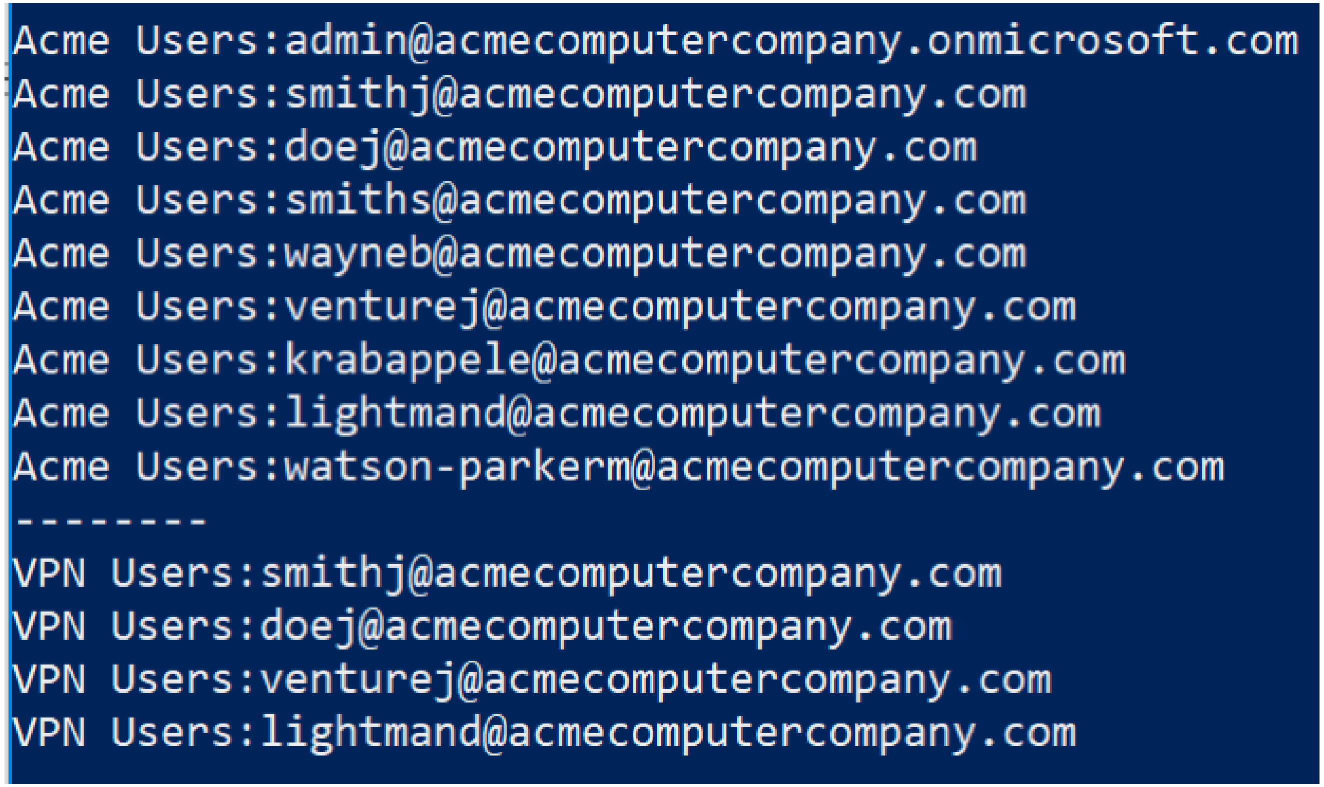


```
Retrieving User List:

UserPrincipalName
-----------------
lightmand@acmecomputercompany.com
smiths@acmecomputercompany.com
wayneb@acmecomputercompany.com
parkerp@acmecomputercompany.com
watson-parkerm@acmecomputercompany.com
venturej@acmecomputercompany.com
smithj@acmecomputercompany.com
testuser@acmecomputercompany.com
doej@acmecomputercompany.com
admin@acmecomputercompany.onmicrosoft.com
krabappele@acmecomputercompany.com
```

Figure 4 – Retrieving User List via o365recon

Now, with a full user list, go back and brute-force again. I've gone from a single credential to hundreds of credentials with a single run (the place had good usernames, bad passwords).

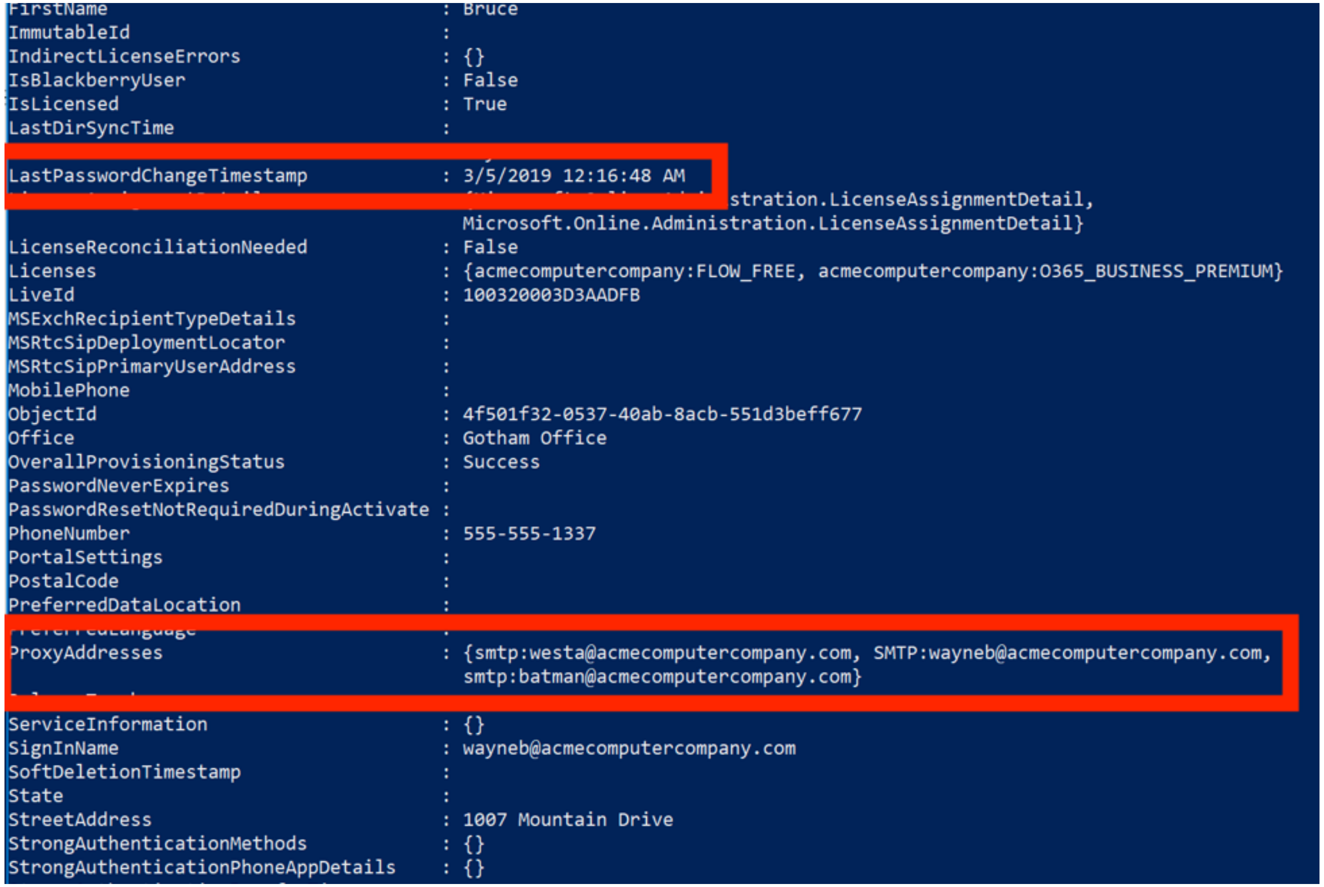


```
Acme Users:admin@acmecomputercompany.onmicrosoft.com
Acme Users:smithj@acmecomputercompany.com
Acme Users:doej@acmecomputercompany.com
Acme Users:smiths@acmecomputercompany.com
Acme Users:wayneb@acmecomputercompany.com
Acme Users:venturej@acmecomputercompany.com
Acme Users:krabappele@acmecomputercompany.com
Acme Users:lightmand@acmecomputercompany.com
Acme Users:watson-parkerm@acmecomputercompany.com
--------
VPN Users:smithj@acmecomputercompany.com
VPN Users:doej@acmecomputercompany.com
VPN Users:venturej@acmecomputercompany.com
VPN Users:lightmand@acmecomputercompany.com
```

Figure 5 – Retrieving Group Membership via o365recon

In addition to group membership, reviewing the full user details can also be helpful. One problem you may encounter is the Active Directory username may not match the email address. For instance, the O365 username may be 'john.smith@acmecomputercompany.com' but the internal username may be

‘LastPasswordTimestamp’ field, which will help you gauge how long your current credentials will work.



```
FirstName                              : Bruce
ImmutableId                            :
IndirectLicenseErrors                  : {}
IsBlackberryUser                       : False
IsLicensed                             : True
LastDirSyncTime                        :

LastPasswordChangeTimestamp            : 3/5/2019 12:16:48 AM
                                                     stration.LicenseAssignmentDetail,
                                         Microsoft.Online.Administration.LicenseAssignmentDetail}
LicenseReconciliationNeeded            : False
Licenses                               : {acmecomputercompany:FLOW_FREE, acmecomputercompany:O365_BUSINESS_PREMIUM}
LiveId                                 : 100320003D3AADFB
MSExchRecipientTypeDetails             :
MSRtcSipDeploymentLocator              :
MSRtcSipPrimaryUserAddress             :
MobilePhone                            :
ObjectId                               : 4f501f32-0537-40ab-8acb-551d3beff677
Office                                 : Gotham Office
OverallProvisioningStatus              : Success
PasswordNeverExpires                   :
PasswordResetNotRequiredDuringActivate :
PhoneNumber                            : 555-555-1337
PortalSettings                         :
PostalCode                             :
PreferredDataLocation                  :
PreferredLanguage
ProxyAddresses                         : {smtp:westa@acmecomputercompany.com, SMTP:wayneb@acmecomputercompany.com,
                                         smtp:batman@acmecomputercompany.com}

ServiceInformation                     : {}
SignInName                             : wayneb@acmecomputercompany.com
SoftDeletionTimestamp                  :
State                                  :
StreetAddress                          : 1007 Mountain Drive
StrongAuthenticationMethods            : {}
StrongAuthenticationPhoneAppDetails    : {}
```

Figure 6 – Retrieving Detailed User Information via o365recon

If you cannot find the internal username via the aforementioned method, you can try to gather them with the ‘Get-ADUsernameFromEWS’ module from MailSniper (https://github.com/dafthack/MailSniper).

Search for single-factor portals. Be aware that their internal username format may not match email address format. Citrix and VPNs are obvious choices. Maybe they have an old OWA server still installed, where it might be possible to use Ruler to get a shell via Homepage attack (https://github.com/sensepost/ruler). At the very least, you might be able to use your valid user account to phish some more powerful users.

You've fought and scrapped, and after some intense brute-forcing, you have gathered a handful of valid usernames and passwords. Now, go forth and plunder.

A Word to the Defenders

How can we stop attackers preying on weak passwords?

The best solution is to enable multi-factor authentication (MFA) for all O365 accounts. Add MFA to everything. If there's something you can't set up with MFA, burn it down, or make it only accessible via VPN (which you also have configured with MFA). If every external-facing portal on your IP space is MFA, then it doesn't matter if an account's password is compromised. Passwords alone are insufficient to protect important external resources.

https://www.microsoft.com/en-us/microsoft-365/blog/2018/03/05/azure-ad-and-adfs-best-practices-defending-against-password-spray-attacks/

Depending on your Office subscription, you may already have access to some tools like Office 365 Advanced Threat Protection. More information can be found here: https://docs.microsoft.com/en-us/office365/securitycompliance/office-365-ti

Finally, check out this great talk by Sean Metcalf that addresses many issues affecting O365 admins, such as getting your logs into your security information and event management (SIEM).

Video: https://www.youtube.com/watch?v=1loGEPn_n7U

Slide Deck: https://adsecurity.org/wp-content/uploads/2019/04/2019-BSidesCharm-YouMovedtoOffice365NowWhat-Metcalf.pdf

MORE LIKE THIS

By Mike Spitzer in Application Security Assessment, Penetration Testing, Security Testing & Analysis

MSBuild: A Profitable Sidekick!

TRUSTEDSEC
Security Blog

Adventures in Phishing Email Analysis

June 18, 2020

By Justin Vaicaro in Incident Response, Incident Response & Forensics, Penetration Testing, Social Engineering, Threat Hunting

14780 Pearl Road, Suite 300
Strongsville, OH 44136

1-877-550-4728

GET TRUSTEDSEC IN YOUR INBOX

Sign up to receive the latest in cybersecurity news and resources

By submitting this form, I agree to receive marketing communications from TrustedSec, which I can unsubscribe from at any time.

SUBMIT

Privacy Policy Sitemap

This site is protected by reCAPTCHA and the Google Privacy Policy and Terms of Service apply.