Red Teaming Microsoft: Part 1 - 通过Azure导致Active Directory泄漏

一叶飘零 / 2018-10-30 07:38:00 / 浏览数 2329 技术文章 技术文章 顶(0) 踩(0)

前言

我们已经拥有了很多的Microsoft技术，服务，应用程序以及配置，这将会给管理带来很大的困难。现在想象一下，怎样确保其安全性。虽然如果我们将所有东西都移动到云Bullock（@dafthack）的研究一样，当我们将焦点集中在Google上时，我做到了。

我不会误导你，我也不是一个微软的专家。事实上，我对这些产品和服务了解的越多，我就越感到失落。在过去的一年里，我已经能够操纵和改进这些技术，以便从Red team的角度更好地瞄准这些组织，但我仍然努力尝试理解许多不同的概念。这是什么的默认配置？这是默认提供的吗？这和所有东西都同步吗？如果我在这里做出调整，他

微软版图

因此，您已经运行Microsoft Active Directory和Exchange很多年了，但希望快速将Microsoft Office部署给您的员工，同时还想为他们提供访问某些内部应用程序的Webmail门户、Sharepoint和SSO的权限。在该过程中的某个阶段，您决定迁移到Office 365并且一切都运行正常！您的所有用户都可以使用他们的网络凭据进行身份验证，并且他们的电子邮箱运行正常！您是否认为自己仍然是一个预置型的组织，或者您现在是

一个假象的复杂情况

对于管理预置用户，可以使用传统的Microsoft AD。要管理云服务中的用户，您可以利用Azure AD。对于邮件而言，有一个预置的Exchange，但您随时可以在线将电子邮件移动到Exchange。如果你想要全套Office，可以使用Office 365，但我认为在Microsoft多租户环境中，通过Exchange在线路由，你可以在技术上同时使用两者但只需一次付费。由于您支付了Office 365 Business，因此尽管使用GDrive或Box进行企业文件共享，您还可以获得Skype和OneDrive等许多服务。

您注册了一个以sms令牌为默认传递机制的多因素解决方案，但出于某种原因，您的用户仍然可以使用Outlook进行身份验证而无需MFA（主要归因于Microsoft EWS）。总的来说，一切都很顺利，为此我们得感谢`Azure AD Connect`，或者说是`Azure AD`的同步服务，或者我们是否仍在用`Forefront Identity Manager`运行旧式`DirSync`？无论它是什么，它都在运行着，这是最重要的！

进阶

在刚刚举例说明的情况下会产生许多问题，blue team几乎无法防范这么多不同的攻击，包括从远程泄露Active Directory，到绕过甚至劫持用户的多因子身份验证。

了解谁是组织部门内的人员通常是在第三方服务（如LinkedIn或其他OSINT技术）参与的侦察阶段完成的。如果您在内部网络上，那么重新访问此步骤至关重要，因为您需要

但是，如果您不在内部网络但仍需要确定目标对象，该怎么办？甚至如果组织的目标中心被托管在云中并且您实际上从未真正进入内部网络，该怎么办？

通过Microsoft，如果您使用任何云服务（Office 365，Exchange Online等）与Active Directory（on-prem或者in Azure），那么由于Azure AD，攻击者凭借一张证书就可以轻而易举地泄露您的整个Active Directory结构。

步骤1）对您的Webmail门户进行身份验证（即https://webmail.domain.com/）

步骤2）将您的浏览器URL更改为：https■//azure.microsoft.com/

步骤3）从活动会话中选择帐户

步骤4）选择Azure Active Directory然后就可以尽情享用！

这会产生许多坏的情况。例如，如果我们能够导出所有用户和组，我们将拥有一份非常好的员工名单以及他们所属的组的一张列表。我们还可以了解哪些组需要我们登录VPN

Azure AD的另一个好处是它保存了每个用户的设备信息，因此我们可以看到他们在使用Mac，Windows还是iPhone以及他们的版本信息（即Windows 10.0.16299.0）。如果所有的这些您都不是很满意，我们还可以了解所有业务应用程序及其端点，服务主体名称，其他域名，甚至用户可能进入的虚拟资源（即虚拟机，网

更多

作为一个普通用户，对Azure门户进行身份验证的另一个好处是，您可以创建一个后门，我的意思是"访客"帐户，超级方便！

步骤1）单击"Azure Active Directory"

步骤2）单击"管理"项下的"用户"

步骤3）单击"新访客用户"并邀请您自己

根据其配置，它可能会，也可能不会同步回内部网络。事实上，默认情况下创建访客帐户时，我只核实了一个客户，其中Azure AD Connect是双向同步的，它允许访客帐户进行身份认证以及注册一个多因素的设备和内部VPN。这是一个重要的配置组件，因为它可能会造成非常糟糕的结果。

Azure for Red Teams

通过Web浏览器访问Azure门户非常棒，并且这样会有许多非常棒的优势，但我还没有找到直接导出信息的方法。我试图编写一个可以自动验证并且可以自动执行的工具，但这很麻烦，我知道微软通过将所有强大的技术捆绑在一起，已经为我解决了这个问

Azure CLI（AZ CLI）

作为一名Linux用户，我自然而然地倾向于使用AZ CLI。部分原因是我尽可能多地将数据输入到单行中，部分原因是我在.NET中过度地设计了工具。使用AZ CLI是一种快速简便的方法，可以针对Azure的OAUTH进行身份验证，同时还可以快速导出原始数据。在这篇文章中，我们将关注这个解决方案。

Azure Powershell

随着Powershell Empire和MailSniper等强大的Powershell工具的兴起，令我惊讶的是Azure Powershell还没有进入其中任何一个工具。有大量的Active Directory Cmdlet可以与之交互，要启动它，只需安装Azure RM Powershell，然后运行：Connect-AzureRmAccount

Azure .NET

我是那些在Linux上长大但职业生涯的重要时刻都在写C＃的怪异的书呆子之一。因此，让Azure .NET库与Active Directory交互非常令人振奋。我没有过多地研究这些库，但是从更高的层次来看，它们似乎是Active Directory Graph API的某种包装器。

让我们继续挖掘！

正如我之前提到的，我们将专注于使用AZ CLI与Azure进行交互。首先，我们必须与Azure建立一个活动会话。在Red team中涉及使用Microsoft或Google服务的组织，但我很少尝试直接进入内部网络上的shell。我通常会使用我编写的名为CredSniper的工具来获取网络凭证和多因素令牌，

如果基于这样的假设，我们就会假定已经以某种方式获得了有效的证书。

安装AZ CLI

您需要将Microsoft源添加到apt（假设为Linux），安装Microsoft签名密钥，然后安装Azure CLI：

```
AZ_REPO = $■lsb_release -cs■echo“deb [arch = amd64] https://packages.microsoft.com/repos/azure-cli/ $ AZ_REPO main”| sudo tee

curl -L https://packages.microsoft.com/keys/microsoft.asc | sudo apt-key add  -
```

```
sudo apt-get install apt-transport-https

sudo apt-get update && sudo apt-get install azure-cli
```

通过Web Session进行身份验证

正确安装所有内容后，您需要使用已获取的凭据创建与Azure的会话。最简单的方法是在普通浏览器中使用ADFS或OWA进行身份验证，然后：

```
az login
```

这将在本地生成OAUTH令牌，打开浏览器选项卡到身份验证页面，让您根据已经通过身份验证的帐户再次选择一个帐户。选择完了之后，服务器将验证本地OAUTH令牌，除非

读取数据

现在到了我最喜欢的部分！已经有许多技术用于提取先前研究过的GAL，例如在OWA中使用FindPeople和GetPeopleFilter Web服务。这些技术对于red teamers来说是一个很好的资源，但在以下方面确实会有期局限性：比如有哪些数据是可用的，列举用户需要多长时间，根据Web请求数量确定我们需要多大的空间以及它们 CLI，就可以非常轻松地提取每个用户的所有目录信息。在下面的示例中，我应用JMESPath过滤器来提取我需要的数据。我也可以将其导出为表格，JSON或TSV格式！

所有用户

```
az ad user list --output=table --query='[].{Created:createdDateTime,UPN:userPrincipalName,Name:displayName,Title:jobTitle,Depa
```

特定用户

如果您知道目标帐户的UPN，则可以通过传入-upn标志来检索特定帐户，您也可以很方便地深入了解特定帐户的Active Directory信息。在下面的示例中，您将注意到我提供了JSON格式而不是table output。

```
az ad user list --output=json --query='[].{Created:createdDateTime,UPN:userPrincipalName,Name:displayName,Title:jobTitle,Depar
```

实用命令

下一个我最喜欢的功能是转储组的能力。了解如何在一个组织中发挥一个团队的作用可以帮助我们深入了解业务，用户以及管理员身份。AZ CLI提供了一些有用的命令，可以在这里提供帮助。

所有团体

我通常做的第一件事就是导出所有组。然后我可以找到某些关键字：管理员，VPN，财务，亚马逊，Azure，Oracle，VDI，开发人员等。虽然有其他组元数据可用，但我倾

```
az ad group list --output=json --query='[].{Group:displayName,Description:description}'
```

特定小组成员

一旦你审查了这些小组并挑选了其中一些较为有趣的小组，这将为您提供一个很好的目标列表，这些目标是这些有趣的群体的一部分,与流行的观点不同，我发现技术能力和 / GitLab代码存储库，Jenkins为shell构建服务器，OneDrive / GDrive文件共享敏感数据，Slack团队负责敏感文件和一系列其他第三方服务。再强调一次，如果你不需要的话就没有必要进入内部。

```
az ad group member list --output=json --query='[].{Created:createdDateTime,UPN:userPrincipalName,Name:displayName,Title:jobTit
```

应用程序

Microsoft提供的另一个不错的特点是能够注册使用SSO / ADFS或与其他技术集成的应用程序。许多公司将其用于内部应用。这对于red teamers来说是非常棒的，因为与应用程序相关联的元数据可以帮助我们更深入的了解在侦察期间可能尚未发现的攻击面，例如URL。

所有应用

```
az ad app list --output=table --query='[].{Name:displayName,URL:homepage}'
```

具体应用

在下面的屏幕截图中，您可以看到我们通过检查与Azure中已经注册的应用程序相关联的元数据来获取Splunk实例的URL。

```
az ad app list --output=json --identifier-uri='<uri>'
```

所有服务负责人

```
az ad sp list --output = table --query ='[]■{Name■displayName■Enabled■accountEnabled■URL■homepage■Publisher■publisherName■Me
```

特定服务负责人

```
az ad sp list --output = table --display-name ='<display name>'
```

使用JMESPath进行高级过滤

在上面的示例中您可能已经注意到我尝试限制返回的数据量，这主要是因为我仅仅想获取我所需要的，而不是所有的信息。AZ CLI处理此问题的方法是将-query标志与JMESPath查询一起使用，这是用于与JSON交互的标准查询语言。在将查询标志与show内置函数结合使用时，我注意到了一些AZ CLI的错误使用。另一个需要注意的是，默认的响应格式是JSON，这意味着如果您打算使用查询过滤器，则需要明确正确的区分大小写的命名约定。不同格式的名称之间存

禁止访问Azure Portal

我花了一些时间试图弄清楚要禁用的内容，如何防止访问，如何限制，监控什么，甚至在Twitter上与人联系（在此感谢Josh Rickard！），我感谢所有愿意帮助理解这种疯狂行为的人。我想为了能提供更好的建议，我应该更多地学习微软生态系统。在此之前，我为您提供了一种禁用Azure Portal访问用户的方法。我没有对此进行测试，也无法确定这是否包括AZ CLI，Azure RM Powershell和Microsoft Graph API，但它绝对会是一个开始。

步骤1）使用Global Administrator帐户https://portal.azure.com登录Azure

步骤2）在左侧面板中，选择"Azure Active Directory"

步骤3）选择"用户设置"

步骤4）选择"限制对Azure AD管理门户的访问"

另一种方法是查看Conditional Access Policies：https■//docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview

期待

有许多不同的工具可用于测试AWS环境，甚至是最近出现的用于捕获SharpCloud等云凭据的新工具，云环境似乎是一个常被忽视的攻击面。

我将发布一个（目前是私有的）red team框架，用于与云环境进行交互，称为CloudBurst。它可以使用户能够与不同的云供应商进行交互，从而获取，攻击和泄露数据。

■■■■■https://www.blackhillsinfosec.com/red-teaming-microsoft-part-1-active-directory-leaks-via-azure/

上一篇：SECCON 2018 - PW... 下一篇：2018web安全测试秋季预选赛W...

1. 0 条回复
   - 动动手指，沙发就是你的了！