ROADpersist - Automating Azure Penetration Testing

Becca Fried
Rochester Institute of Technology
Rochester, New York
btf4645@rit.edu

Shannon McHale
Rochester Institute of Technology
Rochester, New York
sxm6549@rit.edu

Julie McGlensey
Rochester Institute of Technology
Rochester, New York
jam9658@rit.edu

Bader Awadh
Rochester Institute of Technology
Rochester, New York
baa7968@rit.edu

ABSTRACT

There has been a rapid migration to the cloud in recent years. With newer platforms like Amazon Web Services (AWS), Google Cloud Platform (GCP), and Microsoft Azure, comes research and tactics to find their flaws. Azure specifically has been an area the cybersecurity community has slowly started making tools for. Our team saw this research as an opportunity to expand our knowledge of Azure and contribute to an existing tool that helps automate the process of penetration testing cloud environments, known as Rouge Office 365 and Azure (active) Directory tools (ROADtools). ROADtools exists as an Azure reconnaissance tool and extracts authentication tokens from the environment. Our offensive plug-in automates tedious tasks often performed by penetration testers after they have used ROADtools to gain access to an Azure AD Environment.

KEYWORDS

Access Tokens, ID Tokens, Microsoft Graph API, MITRE ATT&CK, OAuth, Penetration Test, PowerShell Module, PSGallery, Refresh Tokens.

1 INTRODUCTION

One of the most important components of an Azure penetration test is Azure AD. In fact, The MITRE Corporation has an ATT&CK Matrix specifically for Azure AD. Because cloud and automation are independently becoming the new normal for the cybersecurity field, our group wanted to research both topics. Specifically, we wanted to create or contribute to a tool that automates part of a cloud penetration test. After collecting information on existing tools, we came to the conclusion that we could make the biggest impact on an open-source tool called ROADtools. We learned a significant amount about the authentication process of Azure AD and how ROADtools utilizes it. Finally, we developed our own tool, ROADpersist, as a plug-in for ROADtools to help automate persistence methods identified in the MITRE ATT&CK matrix for Azure.

2 BACKGROUND & SIGNIFICANCE

Cloud computing has taken over the industry. As more and more companies migrate their infrastructures to a cloud model, other parts of the cybersecurity industry will have to adjust. This change will have a huge impact on the way a penetration test is conducted. Microsoft's Azure is the second most popular cloud service in 2021 according to Kinsta [1]. Microsoft has released specific "Rules of Engagement" for penetration testers to follow during their assessments [2]. There have been several open-source tools released following these guidelines to help testers conduct their assessments. Most of these tools, such as BloodHound Azure or Stormspotter, are focused on mapping out the environment to give testers the fastest path to achieve their objective [3][4]. There have not been many tools, however, focused on automating the next steps in the cyber attack lifecycle [5].

2.1 The Cyber Attack Lifecycle

A penetration test usually follows the cyber attack lifecycle in order to be the most successful and effective. The eight steps in the cycle are as follows: initial reconnaissance, initial compromise, establish foothold, escalate privileges, internal reconnaissance, move laterally, maintain persistence, and complete mission [6]. Initial reconnaissance is used to identify exploitable vulnerabilities and determine attack methodology through research. Initial compromise is used to gain initial access into the target. Establish foothold is used to strengthen your position within the target by maintaining control over the target. Escalate privileges is used to steal valid user credentials to gain access to systems and data. Internal reconnaissance is used to identify target data and improve the attack methodology. Move laterally is used to move throughout the target system and identify more targets. Maintain persistence is used to ensure continued access to the target environment. Complete mission is to package and steal the target data, without losing access to the system [7]. The cycle can continue after maintaining persistence if the penetration tester is able to escalate more privileges

and move to other possible vulnerable services. Using the ROADtools suite in a penetration test can help the tester with escalating privileges and internal reconnaissance within an Azure environment, shown in red in Figure 1.

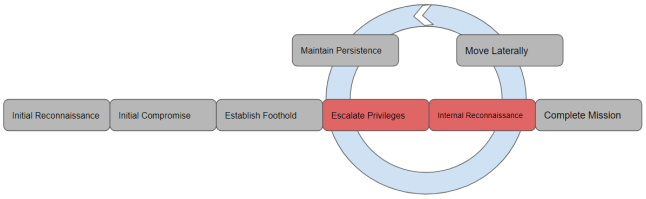

Figure 1: Attack Lifecycle with ROADtools

Using the ROADpersist plug-in as a part of ROADtools can help the penetration tester with maintaining persistence and establishing footholds, shown in green in Figure 2. How this is achieved is discussed more in Section 4.

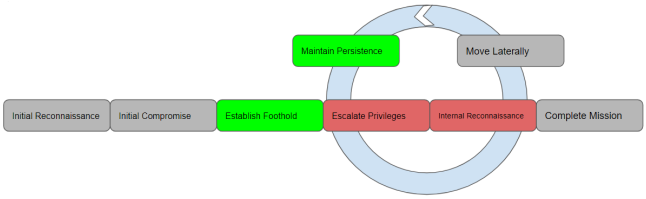

Figure 2: Attack Lifecycle with ROADtools and ROADpersist

2.2 The MITRE ATT&CK Matrix for Microsoft Azure

The MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) Matrix is a framework which lists common tactics, techniques, and procedures (TTPs) used against different environments and platforms [8]. It visualizes the relationship between TTPs which organizations can use to improve detection and analytics, threat intelligence, adversary emulation and red teaming, assessment and engineering, and many other use cases [9]. ATT&CK for Enterprise focuses on adversarial behavior in operating systems like Windows, MacOS, and *nix, along with cloud environments like AWS, GCP, and Microsoft Azure. We chose to reference the Azure platform matrix throughout the tool's development so it would include the most possible techniques attackers might use.

Tactics in the Azure platform matrix include Initial Access, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Collection, Exfiltration, and Impact [10]. We focused on Persistence - hence the name "ROADpersist" - when creating the tool and its scripts. Persistence is defined as "the adversary trying to maintain their foothold" [11]. There are three techniques within the Persistence tactic: Account Manipulation, Create Account, and Valid Accounts. Each technique has at least one sub-technique. During our research and development of the tool, we realized that the Azure ATT&CK matrix seemed to lack some techniques. This is discussed more in Section 5.2.

3 RELATED WORK

3.1 ROADtools

When a user interacts with Azure, they will use a browser-based portal, Azure PowerShell, Azure command-line interface (CLI) or a REST API. All of these interactive options must go through the Azure Resource Manager (ARM) before using any Azure Resources. ARM is the single management endpoint for the Azure platform. It authenticates by checking Azure AD for valid users and their permissions.

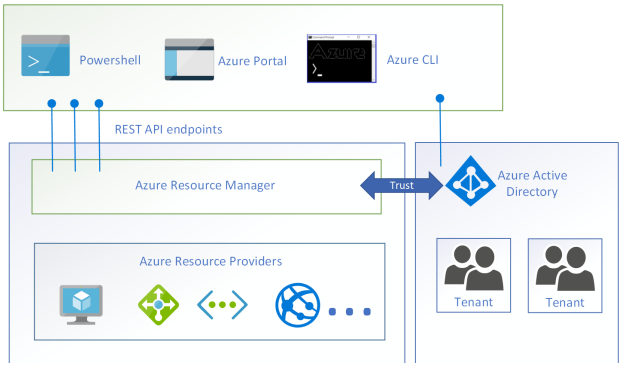

Figure 3: Azure Active Directory diagram

A penetration tester has the ability to abuse the Azure AD authentication process to gain initial access. This can be accomplished by using ROADtools. Once access is granted the penetration tester should try to establish persistence. Our offensive plug-in to ROADtools automates persistence tasks.

3.2 Authentication Tokens

Separate concepts that relate to this tool include token types. Azure has three different token types; ID, access, and refresh. Within Azure, access tokens, which are also JSON Web Tokens (JWT), are used in order to discover its granted permissions. These types of tokens are not encrypted and provide both resource servers and APIs with access. Validation is needed to prove if it is authentic so the signature is analyzed [12].

Refresh tokens are used in order to securely obtain new access and ID tokens from an OAuth 2.0 flow. OAuth is used to both authorize and authenticate many different types

of applications, such as natively installed applications and web applications [13]. Azure Active Directory Business-to-Consumer (Azure AD B2C), is used to safely support many different users with even more authentications. While refresh tokens are alive for quite some time, they can be invalidated for many different reasons. Requesting a token from Azure AD B2C is the only way to fully validate if a refresh token is still valid or not, which in turn provides a new token [14]. In order to maximize the life of refresh tokens, the newest token should replace the older one. This will also improve its security because the longer a refresh token is active, risk and likelihood of an attack increase.

4 OUR TOOL - ROADPERSIST

We contributed to the ROADtools tool suite by creating ROADpersist. ROADpersist is a PowerShell module that utilizes the information gathered in ROADrecon to take the next step in the ATT&CK lifecycle. The plug-in that connects ROADpersist to the ROADtools suite is written in Python. In Azure AD, it has the ability to create new users, add credentials to service principals, and add users to specific roles.

4.1 PowerShell Module

Windows PowerShell modules give users the ability to create a set of related scripts and easily distribute them. Our PowerShell module, ROADpersist, consists of three (3) parts [15].

(1) A manifest file (.psd1) that describes the above files, as well as stores metadata such as author and versioning information.
(2) A .psm1 file containing the functions, or scripts, that ROADpersist allows users to run
(3) A directory that contains all of the above content, and is located where PowerShell can reasonably find it.

By using a PowerShell module to perform actions of persistence we add a greater level of usability. First, our module is hosted on the official Microsoft PowerShell Gallery website [16]. This allows users to easily install our tool using the "import-module roadpersist" command. Second, when a script requires arguments, it prompts the users for them one-by-one using their name such as "password: ". Finally, there is a "help" feature that outlines the functionality of the code and details on the required arguments.

4.2 PowerShell Scripts

ROADpersist has three working PowerShell scripts that each allow a different aspect of persistence. The first script adds a user to the existing Azure AD environment. The second script adds a role to an existing user. The third script adds new credentials in the form of a self signed certificate to an existing service principal.

To add a user to the existing Azure AD environment, the user needs to provide four parameters: a display name, nickname, password, and email address for the new user. The script will then add a new user with the given parameters.

To assign a new role to an existing user, the user needs to provide four parameters: the sign-in name, role definition name, subscription ID, and resource group name. Then, going through the subscription and resource group, a new role will be added to the user. If the user already has a role, the role will not be overwritten. Rather, another role will simply be added to the user. If a penetration tester has control over a user with administrator permissions, they can then alter the access for different users which results in privilege escalation.

Finally, to add new credentials to an existing service principal, the user needs to provide two parameters: the service principal name and certificate name. The script will create a new self-signed base64 encoded public X509 certificate and adds it to the designated service principal.

4.3 Leveraging ROADtools

The ROADtools workflow is broken down into two parts. The first part is the reconnaissance of the target system, done by ROADrecon, and the second part is processing the data and storing it on the host system disk, done by ROADlib. In ROADpersist, we can interact with the SQL database generated by ROADtools directly and parse it to extract the data relevant to our tool workflow.

4.4 Benefits

ROADpersist has the ability to execute most of the persistence techniques listed in the ATT&CK matrix. The Account Manipulation technique has a sub-technique called Additional Cloud Credentials. This is accomplished through a script which add credentials to an existing service principal. The Create Account technique has a sub-technique known as Cloud Account. This is accomplished through a script which creates a new cloud account in the existing Azure AD environment. See Figure 4 for the list of persistence techniques in the ATT&CK matrix. The green cells are ones completed by ROADpersist.

5 FUTURE WORK

In the future, there are some features that would be beneficial to explore. The first would be additional TTPs from the MITRE ATT&CK Matrix. In Figure 5, completed steps are highlighted in green and desired next steps in blue. Additional scripts could be written, starting with the last two sub-techniques left under Persistence: Default Accounts and Cloud Accounts. Adding a connection to the Microsoft Graph API would be very useful when attempting to access information through efficient and flexible queries. We made some

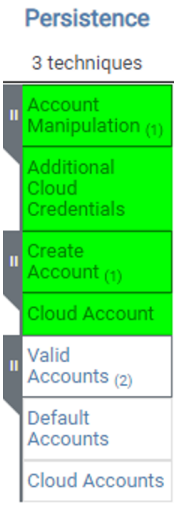

Figure 4: ATT&CK Matrix for Azure - Persistence techniques

progress on this but were unable to complete the connection scripts due to time restraints. Other APIs to explore include Microsoft 365 applications, Microsoft Teams, and Microsoft Exchange. Finally, it would be beneficial to work with Azure CLI more as it can lead to a faster recovery time.

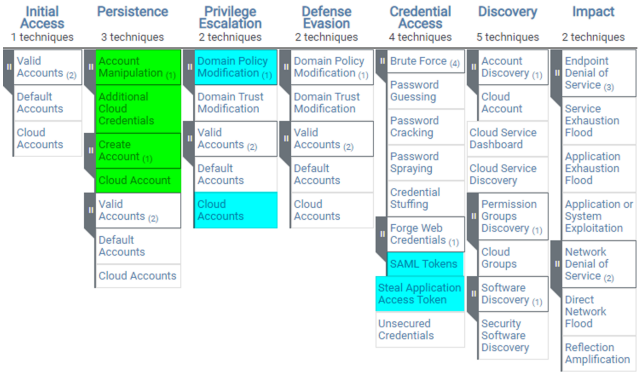

Figure 5: MITRE ATT&CK Mapped to ROADpersist Present and Future

5.1 Weaknesses

Running PowerShell scripts in an Azure environment is bad practice for a penetration tester who wants to perform a stealthy assessment. There are security measures in place to detect when PowerShell is run in an environment and if it is executed by a user that normally does not use PowerShell, it is even more suspicious. This is a point of weakness in the ROADpersist tool. It would be more beneficial if these scripts were written in a more unassuming language like Python.

However, Azure has specifically designed Azure AD to not be compatible with Python. During our development process we created a PowerShell CLI that could execute individual PowerShell scripts using the subprocess command. Unfortunately, the subprocess of PowerShell would occur in a different PowerShell session, thus forcing us to re-authenticate. Instead of having the user log in every time they ran a command, we chose to transition the CLI to a PowerShell module.

Future research may include developing Python code that can interact with Azure AD to add users and perform other actions. This might be possible by interacting through the web API.

5.2 Adjusting The MITRE ATT&CK Matrix

While researching and writing persistence scripts for the Azure environment, we realized that the MITRE ATT&CK Azure matrix seemed to lack some relevant persistence techniques. For example, adding scheduled jobs can be used by adversaries to insert malicious code [17].

Our recommendation is to continue updating the TTPs based on existing cybersecurity incidents. We also believe when the TTPs are clicked on for further information, they should contain incidents pertaining to the cloud environment the matrix was based on. Several times during our research it would lead us to techniques and sub-techniques that were not relevant to cloud environments at all. This requires the work of the entire ATT&CK community, not just The MITRE Corporation.

6 REPOSITORY

In order to view the ROADpersist source code, follow this link to access the repository: https://github.com/Littlehack3r/ROADpersist.

7 ACKNOWLEDGEMENTS

Our group would like to thank Rochester Institute of Technology for the opportunity to pick our research project during our final semesters of school. By allowing us to focus on an area we are passionate about, we were able to produce better work. We would also like to thank our advisor, Dr. Justin Pelletier, for guiding us throughout this semester. We especially appreciate his effort to receive funding for this project. Additionally, we would like to thank The Eaton Cybersecurity SAFE Lab for sponsoring our project and allowing us to further research and complete our tool. Finally, we would like to express our gratitude to Dirk-jan Mollema, the author of ROADtools, for answering our questions and giving us direction for our project.

REFERENCES

[1] E. Jones, "Cloud market share – a look at the cloud ecosystem in 2021," Mar 2021. [Online]. Available: https://kinsta.com/blog/cloud-market-share/

[2] "Microsoft cloud penetration testing rules of engagement." [Online]. Available: https://www.microsoft.com/en-us/msrc/pentest-rules-of-engagement

[3] SpectorOps, "Bloodhoundad/bloodhound." [Online]. Available: https://github.com/BloodHoundAD/BloodHound/blob/master/Collectors/AzureHound.ps1

[4] Azure, "Azure/stormspotter." [Online]. Available: https://github.com/Azure/Stormspotter

[5] "Cyber attack lifecycle," Oct 2015. [Online]. Available: https://www.iacpcybercenter.org/resource-center/what-is-cyber-crime/cyber-attack-lifecycle/

[6] FireEye, "Red team operations data sheet," 2019. [Online]. Available: https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/pf/ms/ds-red-team-operations.pdf

[7] L. E. C. Center, "Cyber attack lifecycle," Oct 2015. [Online]. Available: https://www.iacpcybercenter.org/resource-center/what-is-cyber-crime/cyber-attack-lifecycle/

[8] B. Strom, "Att&ck 101," Sep 2018. [Online]. Available: https://medium.com/mitre-attack/att-ck-101-17074d3bc62

[9] MITRE, "Getting started | mitre att&ck®." [Online]. Available: https://attack.mitre.org/resources/getting-started/

[10] ——, "Azure matrix - enterprise | mitre att&ck®," Oct 2020. [Online]. Available: https://attack.mitre.org/matrices/enterprise/cloud/azure

[11] ——, "Persistence, tactic ta0003 - enterprise | mitre att&ck®," Jul 2019. [Online]. Available: https://attack.mitre.org/tactics/TA0003/

[12] Microsoft, "Overview of tokens in azure active directory b2c," Aug 2020. [Online]. Available: https://docs.microsoft.com/en-us/azure/active-directory-b2c/tokens-overview

[13] ——, "Microsoft identity platform and oauth 2.0 authorization code flow," Mar 2021. [Online]. Available: https://docs.microsoft.com/en-us/azure/active-directory/develop/v2-oauth2-auth-code-flow

[14] ——, "What is azure active directory b2c?" Sep 2019. [Online]. Available: https://docs.microsoft.com/en-us/azure/active-directory-b2c/overview

[15] Joeyaiello, "Understanding a windows powershell module - powershell," Sep 2016. [Online]. Available: https://docs.microsoft.com/en-us/powershell/scripting/developer/module/understanding-a-windows-powershell-module?view=powershell-7.1

[16] "Roadpersist." [Online]. Available: https://www.powershellgallery.com/packages?q=roadpersist

[17] A. Homewood, L. Loobeek, P. Verma, and T. Smith, "Scheduled task/job, technique t1053 - enterprise | mitre att&ck®," May 2017. [Online]. Available: https://attack.mitre.org/techniques/T1053/