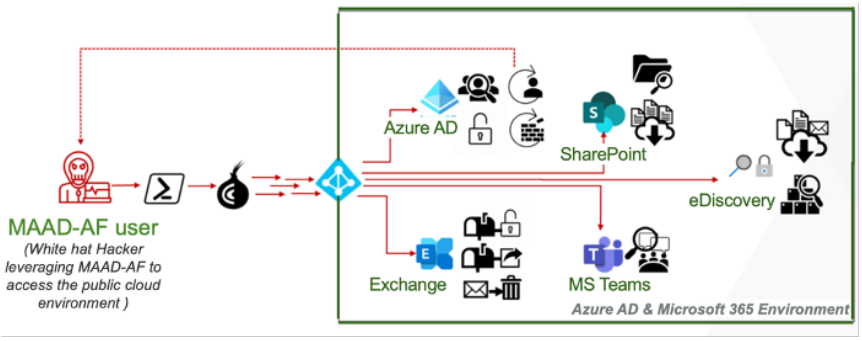
MAAD-AF Opensource Cloud Attack Framework

MAAD-AF is an open-source cloud attack framework developed to test the security of Microsoft 365 & Azure AD environments through adversary emulation. MAAD-AF offers various attack modules to exploit configuration flaws across different Microsoft cloud services & tools, making it easy to emulate attacker tactics & techniques in a Microsoft cloud environment.



With access, MAAD-AF allows you to run exploits on any of the services shown.

Installation & Setup

Plug & Play - It's that easy!

1. **Download* the MAAD repository**
2. **Run PowerShell as Administrator**
3. **Navigate to the local MAAD directory**
4. **Run MAAD_Attack.ps1**

PS> cd /MAAD-Attack-Framework;
./MAAD_Attack.ps1

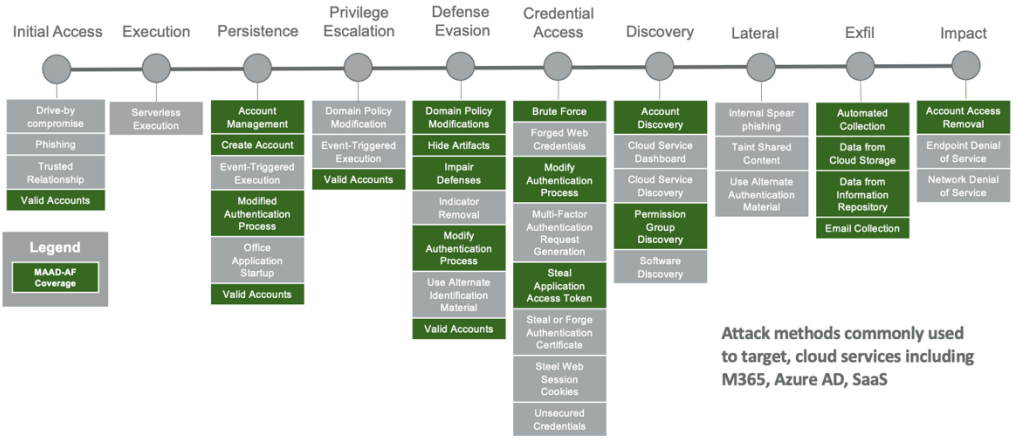
*on windows host

With any of the below MAAD-AF modules, a user can easily and quickly advance related attacks against a specific area of the M365 and Azure AD environment:

Table 1 MAAD-AF Modules for each service

Azure AD	EXCHANGE	TEAMS	SHAREPOINT	eDISCOVERY
— Azure AD Internal Reconnaissance — Azure AD External Reconnaissance — Create Backdoor Accounts — Modify Trusted Network Configuration — Disable MFA — Remove User Access — Brute-Force Credentials	— Disable Mailbox Auditing — Setup Mailbox Rules — Exfiltrate through Mailbox Forwarding — Gain User Mailbox Access — Modify Anti-Phishing Rules	— Recon Internal Teams — Setup External Access to Teams	— Gain Access to SharePoint sites — Search Files & Folders across SharePoint — Recon SharePoint Site Information — Dump Data from SharePoint	— Escalate eDiscovery Privileges — Access & exploit existing eDiscovery searches — Launch searches to collect data — Exfiltrate data using eDiscovery

How MAAD-AF Aligns to MITRE ATT&CK Map



More About MAAD-AF

MAAD-AF source code is developed entirely in PowerShell. It leverages Microsoft APIs to talk to different services and some PowerShell modules to enable its functionality. Each exploit is written as a separate module (contained within the "Library"), making MAAD-AF easily expandable, simple to understand, and easy to contribute to.

MAAD-AF establishes sessions with various Microsoft services using the compromised test credentials supplied by the user. Those sessions are then maintained in the tool and used across the attack modules as necessary. Exploiting the access and privileges of the credentials supplied, users can execute different actions in the Microsoft cloud environment ranging from internal reconnaissance, establishing persistence, privilege escalation, defense evasion, data gathering, and exfiltration.

MAAD-AF is programmed to accept inputs from the user and automatically handle all communication (request & response) with the different Microsoft cloud services. This facilitates ease of use for security teams while offering desired control over the security testing process.

The Future with MAAD-AF

MAAD is open-source, and everyone is invited to use it and contribute to its development.

We are excited about the future of simple and effective security testing. MAAD's features and capabilities will continue to be expanded and improved.

What to expect in future improvements –

- Attack modules for additional Microsoft services
- More modules with attack techniques for existing services
- Source code improvements to make MAAD more modular and easier to add to
- Better reporting capabilities

We must continuously improve and test the security of our cloud environments. We welcome everyone to join MAAD's mission and contribute in any way possible. Send your great ideas, feature requests, report bugs/issues, or contribute directly by writing new attack modules for the MAAD Library.

Get Started Today

While security professionals have limited means to test their Azure AD and M365 security responsiveness against a real attack, MAAD-AF enables them to learn the techniques that attackers perform and emulate how adversaries present in a real environment and how their security solutions can detect or stop an attack. Check out MAAD Github Repository for more information.

Follow the installation and setup steps above and implement Microsoft 365 and Azure AD cloud security testing more easily and quickly.

Here's to making security testing simple, fast, and effective!

Visit www.Vectra.com to learn about solutions that stop attacks on Azure AD or M365