VECTRA

MAAD-AF: Microsoft 365 & Microsoft Entra ID (Azure AD) Attack Framework

Cloud Attack Testing

Don't be the next headline - identify gaps in M365 or Azure AD environments before a breach occurs

Security testing can be challenging, complex, and costly due to the requirement of expertise and the need to avoid impact to infrastructure. The MAAD-AF tool is designed to tackle this challenge by making security testing simple, fast, and effective. It is used by security teams to execute commonly used attack methods by attackers to test cloud security controls. This allows them to have proper visibility to stop an attack.

Key Features:

- **Extensive Testing Coverage:** 30+ attack modules (~50% of MITRE techniques) ranging from initial access, persistence, privilege escalation, defense evasion, credential access, exfiltration, and impact. Effective Testing: Test against techniques frequently used by adversaries & leverage living-off-the-land methods.
- **Ready Out-of-the-Box:** No-setup process. Download and start testing.
- **Intuitive at its Core:** No-commands and a fully interactive prompt-based interface.
- **Clean Testing:** Show your cloud some love – revert most actions executed and keep testing impact to minimal.

Why use MAAD-AF?

- No set up requirements
- Remove complexity with intuitive prompt-based workflows
- 30+ attack modules that can be completed in under an hour
- Effective testing for resilience against the MITRE ATT&CK coverage

READY TO GET STARTED?

Contact us for a MAAD-AF Consultation

info@vectra.ai

https://www.vectra.ai/meet/maad-af

MAAD-AF Overview

MAAD-AF's open-source cloud attack framework was developed by Vectra AI to test the security of Microsoft 365 and Microsoft Entra ID (Azure AD) environments through adversary emulation. With MAAD-AF, security teams can easily emulate real attacker tactics and techniques to progress through a compromised M365 and Azure AD environment. This can help identify gaps in existing configurations and detection and response capabilities to ultimately harden the cloud environment's security.

Requirements

- Window 10/ Window 11 Operating System
- PowerShell Version 5
- Permission to run unsigned PowerShell script
- Internet connectivity and ability to access the Azure AD tenant from host
- If EDR is present, then ideally ability to disable EDR or whitelist MAAD-AF in EDR.
- Local Admin Permissions to use PowerShell as Admin

Recommended Roles for Testing Credentials

Users can test using any credential with any role assignment in Microsoft Entra ID (Azure AD). However, the role assignment will define the scope of testing. In general, the lower the role, fewer techniques can be executed using the test credentials.

Resources

Get the MAAD-AF tool: https://github.com/vectra-ai-research/MAAD-AF

Additional information on MAAD – AF tool: https://openrec0n.github.io/maad-af-docs/

MAAD-AF Attack Lab Webinar: https://info.vectra.ai/are-you-prepared-for-an-identity-based-attack

Contact us for a MAAD-AF Consultation

About Vectra AI

Vectra AI is the leader in hybrid cloud threat detection and response. Vectra's patented Attack Signal Intelligence detects and prioritizes threats across public cloud, SaaS, identity, and networks in a single platform. Vectra's Attack Signal Intelligence goes beyond simple anomaly detection to analyze and understand attacker behavior. The resulting high-fidelity signal and deep context enables security operations teams to prioritize, investigate and respond to cyber-attacks in progress sooner and faster. Organizations worldwide rely on the Vectra platform and MXDR services to stay ahead of modern cyber-attacks. Visit www.vectra.ai.

For more information please contact us:
Email: info@vectra.ai | vectra.ai