Security Monitoring of Active Directory Environment Based on Machine Learning Techniques

Author: Lukáš Kotlaba Supervisor: Ing. Simona Buchovecká, Ph.D.

Department of Information Security, Faculty of Information Technology, Czech Technical University in Prague

FACULTY OF INFORMATION TECHNOLOGY CTU IN PRAGUE

Motivation

Active Directory is a central point of administration and identity management in many organizations. Ensuring its security is indispensable to protect user credentials, enterprise systems, and sensitive data from unauthorized access.

Security monitoring of Active Directory environments is typically performed using signature-based detection rules. Those, however, often result in a high number of false alerts. This work utilizes machine learning techniques to improve detection capabilities, and at the same time, reduce the number of false alarms in comparison with traditional detection mechanisms.

Active Directory Background

Active Directory (AD):

- is a directory service from Microsoft, broadly adopted by organizations,
- stores information about objects on a domain network, such as users, groups, computers, and many others, together with their attributes,
- is typically used for a broad range of identity services, basic examples of which are authentication and authorization for users and computers.

Considering the type of data stored in AD, it is not surprising that it represents an interesting target for cyber attackers. Once adversaries get access to AD, the consequences can be fatal, even resulting in full domain compromise.

Security Monitoring

Traditional detection of AD attacks is based on a rule-based analysis of Windows Event Log events. Detection rules contain specific conditions that are checked against log data collected from machines over the network. If the defined conditions are matched, the rule is triggered, and an alert is generated. **This work applies machine learning techniques to improve the detection logic.**

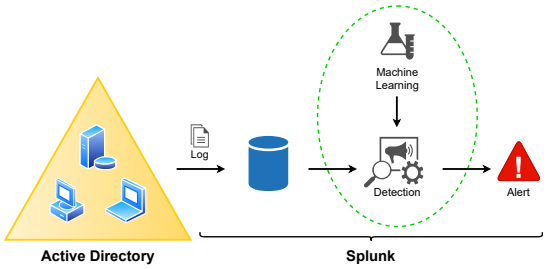

Figure 1. Security monitoring architecture

To reflect a real-life scenario, auditing data from a real Active Directory environment was used. The designed detection methods were implemented in Splunk, a commercial tool commonly used for security monitoring.

Selected Attack Techniques

Based on research of existing detection approaches, two adversary techniques for which signature-based detection is not sufficient were selected:

Password Spraying

- type of brute force attack on users' passwords
- a single password is attempted towards many user accounts

Kerberoasting

- attacker obtains authentication ticket towards a remote service
- if the ticket is cracked, password of the service account is discovered

Both selected attacks share common properties:

- the attacks are relatively easy for an attacker to execute,
- are typically detected using threshold rules,
- it is difficult to distinguish an attack from regular user activities.

Machine Learning Algorithms

In general, two detection approaches for security monitoring can be identified:

- **misuse detection** that models abnormal behavior based on known attacks,
- **anomaly detection** that models normal behavior and looks for deviations.

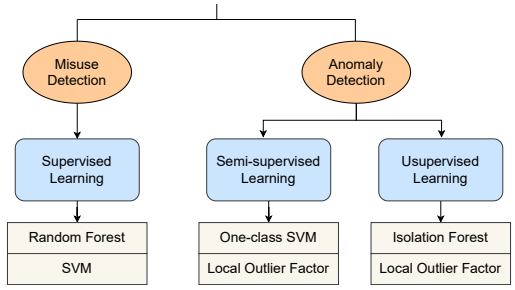

Figure 2. Machine learning techniques applied

This work utilized different machine learning (ML) approaches (unsupervised, semi-supervised, and supervised) and aimed to find the most suitable method for detecting the selected attacks. Two representative algorithms were chosen and evaluated for each category.

While applying machine learning algorithms to this task, great emphasis was put on the feature engineering step. The majority of data fields contained in Windows events cannot be used directly as features in machine learning models, as those usually require numeric features.

Results

Performance of the proposed ML solutions was compared to the traditional rules designed to detect the selected attack techniques that contained threshold conditions. The results are presented in terms of the confusion matrix concept, commonly used in both ML and security monitoring fields. The figures below show the results of the methods evaluated as the best based on the experiments.

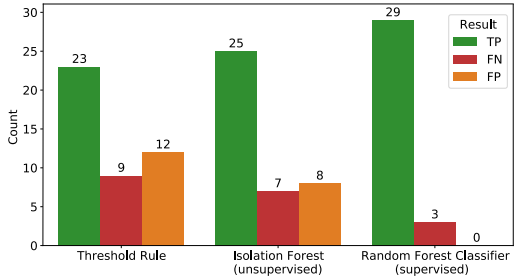

Figure 3. Results of **Password Spraying** detection

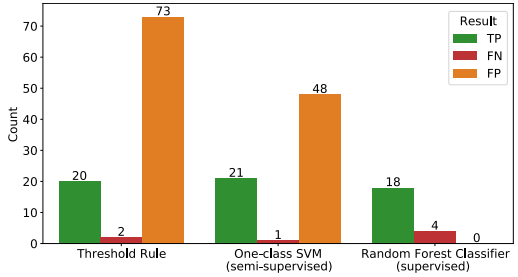

Figure 4. Results of **Kerberoasting** detection

Conclusions

Machine learning approaches were able to improve detection characteristics for both researched attack techniques in comparison with the threshold rules. The number of false alarms was significantly reduced, and several attacks otherwise missed by the threshold rules were detected.

Outputs of this work include:

- two Splunk ML-based detection rules for each attack technique that are directly applicable in practice,
- comprehensively documented ML analysis process aiming to help future development of ML-based detections in AD environments.