УДК 004.056.5

СИСТЕМА МОНИТОРИНГА СОБЫТИЙ ИБ В ACTIVE DIRECTORY

Смалько В.П.

гр.367241

Белорусский государственный университет информатики и радиоэлектроники,
г. Минск, Республика Беларусь

Научный руководитель: Борботько Т.В. – доктор технических наук, профессор, зав. кафедры ФИБ

Аннотация. Противодействию нарушителю в информационных системах основанных на

использовании контроллеров доменов обусловлено обнаружению событий информационной безопасности, возникающих в них при кибератаке. Такого рода воздействия являются разрушительными и приводят к неприемлемому ущербу. Поэтому мониторинг подобного рода событий является обязательным процессом в управлении информационной безопасностью организации.

Ключевые слова: события ИБ, система мониторинга, Active Directory, MITRE ATT&CK

Введение. В условиях современной информационной среды одним из ключевых аспектов обеспечения безопасности корпоративных информационных систем является эффективное мониторинг и реагирование на события, связанные с информационной безопасностью. Active Directory (AD) как центральная служба управления доступом и идентификации в корпоративных сетях, подверженный различным угрозам, становится объектом повышенного внимания вопросов информационной безопасности.

Целью исследования является анализ кибератак на AD и разработка системы мониторинга событий ИБ в AD. В работе будут рассмотрены основные этапы кибератаки на AD в соответствии с MITRE ATT&CK, основные техники, используемые нарушителями, а также различные виды кибератак на AD. Затем будет представлена разработка системы мониторинга событий ИБ в AD, включая ее цели, задачи и методы в соответствии с MITRE ENGAGE.

Основная часть. Каждая кибератака на Active Directory может быть разделена на несколько этапов, которые злоумышленники используют для достижения своих целей. MITRE ATT&CK Framework определяет эти этапы, предоставляя систематизированный подход к анализу кибератак и улучшению систем защиты, состоящий из тактик и техник (рисунок 1).

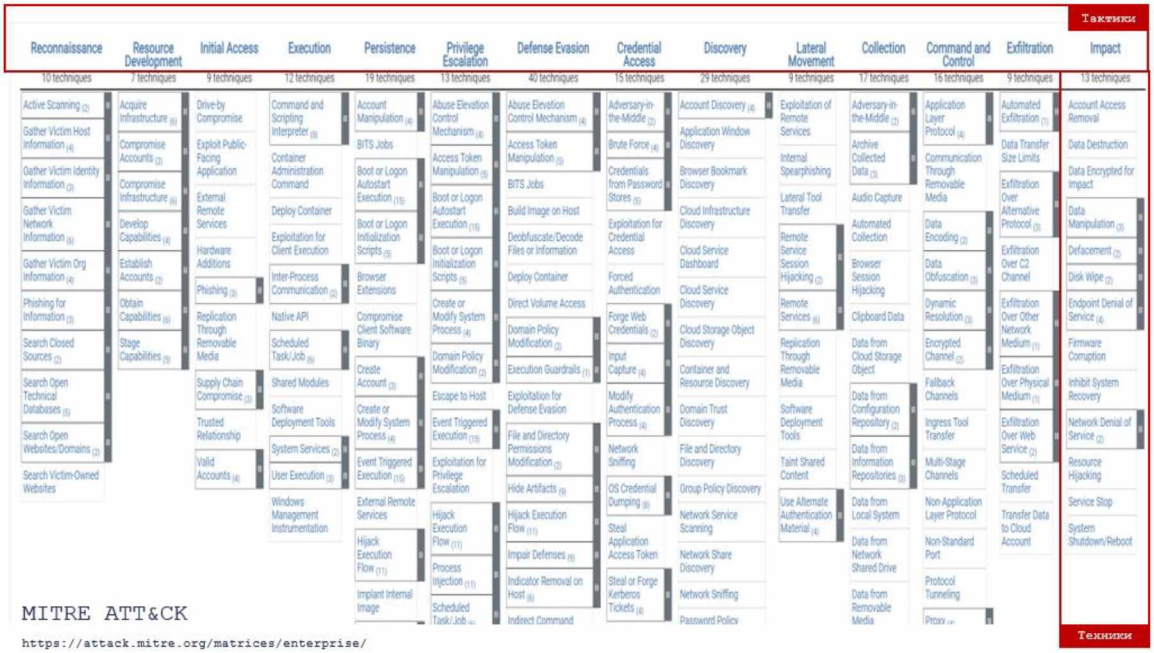

Рисунок 1 – матрица MITRE ATT&CK

На этапе разведки (Reconnaissance) злоумышленники исследуют AD, собирая информацию о пользователях, группах и ресурсах. Например, сканирование SPN (Service Principal Names), сбор данных из общих ресурсов - сетевые папки, файловые сервера, базы данных, NAS (Network Attached Storage), а также такие пользовательские данные (при

наличии привилегий) как учетные данные пользователей, локальные данные, пользовательские файлы. При наличии привилегий, Microsoft Exchange и Outlook также могут быть скомпрометированы [1].

На этапе разработка ресурсов (Resource Development), злоумышленники создают или компрометируют учетные записи и другие ресурсы, которые будут использоваться для атаки на AD. Это может включать в себя создание фальшивых учетных записей или использование украденных учетных данных [2].

На этапе начального доступа (Initial Access), злоумышленники используют различные методы, такие как фишинг или вредоносное ПО, чтобы получить первоначальный доступ к AD. Это может включать в себя отправку фишинговых писем с вредоносными вложениями или ссылками [2].

На этапе выполнения (Execution), злоумышленники выполняют вредоносный код или ПО на скомпрометированной системе. Это может включать в себя использование скриптовых языков, таких как PowerShell, для выполнения вредоносного кода [2].

На этапе закрепления (Persistence), **злоумышленники используют различные** методы, чтобы сохранить свой доступ к AD. Это может включать в себя создание служб Windows или заданий планировщика, которые автоматически запускают вредоносный код при каждом входе в систему [2].

На этапе эскалации привилегий (Privilege Escalation), злоумышленники используют различные методы, чтобы повысить свои привилегии в AD. Это может включать в себя извлечение пароля локального администратора из SYSVOL (общедоменный ресурс Active Directory, к которому у всех авторизованных пользователей есть доступ на чтение. SYSVOL содержит сценарии входа, данные групповой политики и другие данные, которые должны быть доступны везде, где распространяется политика домена.), также возможно использование метода делегирования Kerberos, загрузка dll библиотеки на DNS-сервер пользователем, входящим в группу DNSAdmins или обладающим правами на запись в объекты DNS-сервера и др. методы [1].

На этапе обхода защиты (Defense Evasion), злоумышленники используют различные методы, чтобы избежать обнаружения. Это может включать в себя отключение антивирусного программного обеспечения или изменение настроек безопасности [2].

На этапе доступа к учетным данным (Credential Access), злоумышленники используют различные методы, чтобы получить доступ к учетным данным. Это может включать в себя кражу хэшей паролей или билетов Kerberos, получение копии файла ntds.dit (база данных, в которой хранится информация Active Directory) [1].

Рассмотренная часть тактик (этапов) показывает, нам что для достижения целей злоумышленник выполняет большое количество операций, которые непременно оставляют следы (артефакты) в системе.

Благодаря найденным артефактам и целям, которые преследует организация при защите своей инфраструктуры может быть использована матрица активной защиты MITRE ENGAGE. MITRE ENGAGE — это платформа для планирования и обсуждения операций по взаимодействию с противником, которая позволяет взаимодействовать с противниками и достигать целей в области кибербезопасности.

. Он основан на простом предположении: поскольку компрометация сети часто неизбежна, защитники могут использовать методологии вовлечения противника, чтобы гарантировать, что компрометация не означает потерю. Вовлечение противника предлагает защитникам возможность увеличить стоимость и уменьшить ценность операций противника. Фреймворк был разработан для обороны от кибератак. Он соответствует фреймворку MITRE ATT&CK, что позволяет специалистам быстро определить уязвимости

злоумышленника при использовании конкретной техники ATT&CK и как использовать эти уязвимости [3].

Для обеспечения более эффективной защиты от киберугроз может быть разработана система мониторинга информационной безопасности Active Directory, основанная на MITRE ATT&CK и MITRE ENGAGE.

Система мониторинга ИБ Active Directory, основанная на матрицах MITRE, может включать следующие компоненты:

- мониторинг аутентификационных сертификатов, который отслеживает запросы сертификатов AD CS (EID 4886), а также выданные сертификаты (EID 4887) на предмет аномальной активности, включая неожиданные регистрации сертификатов и признаки злоупотребления в атрибутах сертификата;
- мониторинг билетов Kerberos, который отслеживает аномальную активность Kerberos, такой как деформированные или пустые поля в событиях входа/выхода из Windows (EID 4624, 4672, 4634), шифрование RC4 в билетах предоставления билетов (TGTs) и запросы билетов предоставления услуг (TGS) без предварительных запросов TGT;
- мониторинг альтернативных материалов аутентификации: отслеживание запросов новых билетов предоставления билетов или билетов на услуги к контроллеру домена, таких как Windows EID 4769 или 4768, которые могут использовать альтернативные материалы аутентификации, такие как хэши паролей, билеты Kerberos и токены доступа к приложениям, чтобы перемещаться по среде и обходить обычные системные контроли доступа.

Заключение. Систем не ограничена описанными компонентами и может быть дополнена. Разработанная система позволит обнаруживать аномалии и подозрительные действия, основываясь на тактиках, методах и процедурах, описанных в матрицах MITRE.

Список использованных источников:

1.Active Directory глазами хакера. – СПБ.: БХВ-Петербург, 2022 – 176с. – Ralf Hacker.

2.Enterprise Matrix [Электронный ресурс]. – Режим доступа: https://attack.mitre.org/matrices/enterprise/. – Дата доступа: 18.02.2024.

3.MITRE Engage: A Framework and Community for Cyber Deception [Электронный ресурс]. – Режим доступа: https://www.mitre.org/news-insights/impact-story/mitre-engage-framework-and-community-cyber-deception. – Дата доступа: 18.02.2024.

UDC 004.056.5

INFORMATION SECURITY EVENT MONITORING SYSTEM IN ACTIVE DIRECTORY

Smalko V. P.

gr. 367241

Belarusian State University of Informatics and Radioelectronics,
Minsk, Republic of Belarus

Scientific supervisor: Borbotko T.V. – Doctor of Technical Sciences, Professor, Head of the FIB Department

Annotation. Countering an intruder in information systems based on the use of domain controllers is due to the detection of information security events that occur in them during a cyberattack. Such impacts are devastating and lead to unacceptable damage. Therefore, monitoring of such events is a mandatory process in the management of information security of an organization.

Keywords: information security events, Monitoring system, Active Directory, MITRE ATT&CK.