Emulation of attack techniques to improve the security posture of an infrastructure managed by Active Directory

Armelle Sanya[1,*,†], Max Fréjus O. Sanya[1,†], Emery ASSOGBA[2,†] and Tahirou DJARA[1,†]

[1]Ecole Polytechnique d'Abomey-Calavi (EPAC), University of Abomey-Calavi, Abomey-Calavi, Benin
[2]Institut de Formation et de Recherche en Informatique (IFRI), University of Abomey-Calavi, Abomey-Calavi, Benin

Abstract

Companies and public and private organizations face increasing cyber threats. To combat these threats, they need an effective defense methodology that considers the techniques used by potential attackers. This work involved using the MITRE ATT&CK knowledge base's attack techniques against an infrastructure managed by Active Directory in a contained environment. Three defense profiles based on the state of the art were proposed, and techniques to circumvent them were implemented. Appropriate recommendations for companies and organizations were provided.

Keywords

Active Directory, MITRE ATT&CK, Mimikatz, Attack techniques

1. Introduction

Computer infrastructures are interconnected systems used to store, process, and transmit sensitive information [1]. With the increase in the volume of data processed and stored, these computer infrastructures have gained significant importance, especially with the integration of emerging technologies such as Cloud computing, the Internet of Things (IoT), and social networks. These integrations also unfortunately bring a weakening influence on the security of information systems related to these infrastructures [2].

In Africa, and more specifically in Benin, a digitization effort has been initiated in recent years, along with the establishment of laws and systems to secure these infrastructures. However, the task is enormous, and human and financial resources are scarce. This situation increases the risks associated with the use of digital technology [3].

The security of computer infrastructures is a major concern for cybersecurity professionals due to the significant disruptions and economic damages that cyberattacks can cause. Therefore, it is essential to have a good understanding of the security mechanisms associated with the IT tools used by companies. Notably, 90% of companies use the Active Directory tool [4] for managing user and machine access and permissions. Active Directory is a prime target for attackers seeking to obtain sensitive information or take control of an infrastructure, as it provides and controls access to all of an organization's resources [5]. Attackers constantly seek to exploit vulnerabilities in IT infrastructures to access sensitive information or disrupt business activities.

It is therefore necessary for companies and organizations to gain better knowledge of the potential attacks they might face. For this purpose, the MITRE organization, in collaboration with many other organizations worldwide, has created the MITRE ATT&CK® platform, which lists the techniques used by attackers of information systems. Cybersecurity professionals use it to assess the security posture of organizations' information systems. They can use the techniques listed by MITRE for attack emulation exercises, providing a better view of the security measures applied to these information systems [6].

In the fight against cyberattacks, the main objective of this work is to provide appropriate recommendations to companies and organizations to further secure their information systems. To achieve this, we will explore the techniques listed on the MITRE ATT&CK® platform to simulate attack scenarios against Active Directory managed infrastructures, which will be documented.

2. Literature review

This section presents some concepts related to the study conducted and some work done on the subject.

2.1. Active Directory

The Active Directory tool stores information about network objects and makes it available to users and network administrators so they can find and use it quickly [7].

It allows centralized, secure, and scalable management of resources represented by objects, classified according to their name and attributes. These objects can include users, computers, groups, resources, and other IT infrastructure elements.

2.2. Attack phases against domain environments

Attacks against domain environments typically occur in several stages as shown in Figure 1.

Briefly, these stages are:

1. **Compromise of a domain machine**: This can be done via an open port, an application on the domain, or physical access to the machine.

Cotonou'24: International Conference of Information and Communication Technologies of ANSALB (CITA): Security issues in the age of AI, June 27–28, 2024, Cotonou, BENIN
*Corresponding author.
†These authors contributed equally.
sanyaarmelle@gmail.com (A. Sanya); frejus.sanya@uac.bj (M. F. O. Sanya); assogba.emery@gmail.com (E. ASSOGBA); csmdjara@gmail.com (T. DJARA)

2. **Internal reconnaissance or information gathering**: This is done by executing individual commands or a script to obtain information about the vulnerabilities of the compromised machine.
3. **Local privilege escalation**: This involves exploiting discovered vulnerabilities to gain higher permissions on the machine.
4. **Access to domain administrator credentials**: This involves using tools or scripts to search for domain administrator credentials from the compromised machine.
5. **Action**: Exploiting previously obtained credentials to take control of the domain.

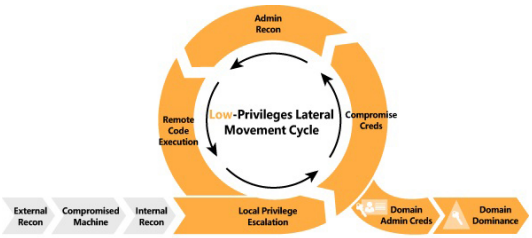

Figure 1: Typical attack chain stages [8].

2.3. Blue and Red Teams

Red teams orchestrate sophisticated attacks to exploit the vulnerabilities of the involved systems [8]. Blue teams, on the other hand, protect digital assets by detecting and neutralizing various attacks from Red teams [9].

Both types of teams play an important role in securing information systems. They help determine essential parameters for the security of information systems, facilitating the role of Information Security Management Systems (ISMS) [10].

2.4. Information System

An information system is a set of interconnected elements whose purpose is to collect, store, process, and disseminate information within the organization or company. It aims to facilitate decision-making processes, optimize internal operations, and improve communication and collaboration [11].

2.5. Related work

Many authors have conducted instructive studies on the attacks targeting infrastructures related to the Active Directory tool.

Among them, Oni Bamidele and Aboubakar Kpelafiya [12] first present the basic architectures of Windows and Linux Active Directory, as well as the related concepts. They then explain the main vulnerabilities observed in these types of infrastructures, along with several attack methods exploiting these vulnerabilities, such as using tools like Powersploit or even Powershell.

From a more general perspective, Mokhtar BI et al. [5] present the attack phases observed at the Active Directory domain level. They explain the most popular types of attacks, such as exploiting the Kerberos authentication protocol. The authors illustrate a typical attack with the test environment set up.

C. D. Motero et al. [13] present a study focused on attacks targeting the Kerberos authentication protocol. This study was conducted by following defined steps, such as setting up a virtual test environment, collecting information about the domain users, gathering tools for various attacks, and documenting these attacks. They add detection and prevention methods specific to the implemented attacks.

Pektaş Abdurrahman, in this article [14], presents penetration testing methods and emphasizes those effective for Microsoft environments.

MITRE ATT&CK® helps to develop threat models and specific methodologies for the private sector, public administrations, and the cybersecurity community, gathering known attack techniques [15].

3. Material and Methods

In this section, we used specific material and several methods.

3.1. Material

We set up a test domain environment using a local network.

Figure 2 shows the material used, as well as the operating systems and users set up on the simulated domain machines.

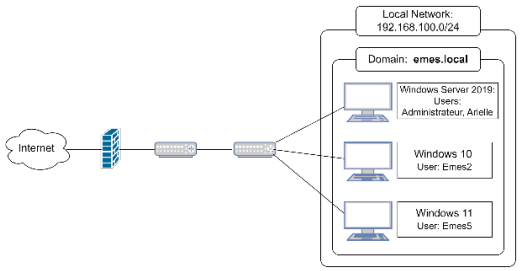

Figure 2: Architecture of the simulation domain environment.

We also used scripts and tools, mainly:

- **PowerUp**: A script that gathers common Windows privilege escalation vectors based on misconfigurations [16].
- **Script.c**: A custom script written in C programming language. It allowed us to implement the privilege escalation phase using a Powershell command. Figure 3 shows the script snippet related to assigning the local administrator role to the compromised user account.
- **Invoke-Mimikatz.ps1**, the Powershell format of Mimikatz [17]: It allows searching and retrieving hashes, clear text passwords, Kerberos authentication tickets, and other user information from the compromised machine.

```
char command[250];
strcpy( command, "powershell.exe Start-Process
powershell.exe -Wait -Verb RunAs -argumentlist '-
noexit Add-LocalGroupMember -Group
\"Administrateurs\" -Member \"Emes\\Emes2\";
timeout /t 3; exit'" );
system(command);
```

Figure 3: Script.c snippet: command executed for privilege escalation.

3.2. Methods

The work highlighted the phases of an attack against a domain environment during a scenario. We started with the following assumptions:

- **H-1**: The administrator has just created the domain, and their primary goal was to allow users to exploit this Active Directory (AD) managed domain for file sharing. The default security mechanisms enabled are Windows Defender antivirus, AMSI (Antimalware Scan Interface), and the firewall.
- **H-2**: The attacker has already compromised a low-privilege account.

We then proceeded with the steps shown in Figure 4 to simulate an attack scenario against the set-up infrastructure.

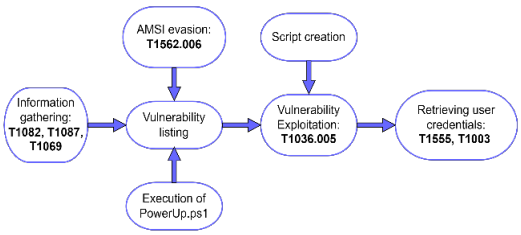

Figure 4: Scenario steps.

The techniques used are respectively:

- **T1082 System Information Discovery** [18]: It involves collecting detailed information about the operating system and hardware, including the version, patches, service packs, and architecture of the compromised machine.
- **T1087 Account Discovery** [19]: It allows obtaining a list of valid accounts, usernames, or email addresses on a system.
- **T1069 Permission Groups Discovery** [20]: It helps determine available user accounts and groups, the membership of users in specific groups, and users and groups with elevated permissions.
- **T1562.006 Impair Defenses: Indicator Blocking** [21]: This involves attempting to prevent the collection and analysis of indicators or events typically captured by sensors such as the Anti-Malware Scan Interface. This technique allowed us to evade antivirus detection during the execution of the used scripts.
- **T1036.005 Masquerading: Match Legitimate Name or Location** [22]: This allowed us to replace a legitimate executable with another file having the same name. The latter resulted from the compilation of the custom script script.c and enabled the elevation of privileges from a compromised standard user to a local administrator.
- **T1555 Credentials from Password Stores** [23] and **T1003 OS Credential Dumping** [24]: We implemented these techniques using the arguments employed during the execution of the Invoke-Mimikatz.ps1 script (figure 5).

```
PS C:\Users\Emes2.EMES\Downloads> Invoke-Mimikatz -
Command '"privilege::debug" "token::elevate"
"sekurlsa::tickets /export" "lsadump::dcsync
/domain:emes.local /all" "lsadump::sam"
"lsadump::cache" "sekurlsa::logonPasswords" "exit"'
| Out-File ret.txt
```

Figure 5: Execution of Invoke-Mimikatz.ps1.

According to this article on the secrets of Mimikatz [17], these arguments correspond to:

- **privilege::debug**: Obtain debugging rights as this access right is necessary for the execution of many Mimikatz commands;
- **token::elevate**: Impersonate a token. It is used to elevate permissions to those of the SYSTEM user or an administrator;
- **sekurlsa::tickets /export**: List all available Kerberos tickets for all recently authenticated users;
- **lsadump::dcsync**: Impersonate a high-privilege user to retrieve the password hashes of domain users from the domain controller;
- **lsadump::sam**: Use the SysKey to decrypt SAM entries. The ”sam” option connects to the local Security Account Manager (SAM) database and extracts the credentials of local accounts;
- **lsadump::cache**: Retrieve user information from the machine's MSCache;
- **sekurlsa::logonPasswords**: List all available logon credential managers. It typically shows the logon credentials of users currently or recently logged into the machine

4. Results and recommendations

This section presents the results obtained and the recommendations given.

4.1. Results obtained at the end of the scenario

At the end of our scenario, we obtained the credentials of users who logged into the domain from the compromised machine.

Figure 6 shows the username and password in MsCache v2 format of these users, as they were found after the execution of the Invoke-Mimikatz.ps1 script.

```
[NL$1 - 06/09/2023 12:03:38]
RID        : 00000457 (1111)
User       : EMES\Emes2
MsCacheV2  : 7a7ef0259b3fa0be24b72898718f14b5

[NL$2 - 06/09/2023 11:53:31]
RID        : 000001f4 (500)
User       : EMES\Administrateur
MsCacheV2  : a211286e4121881de6c026a9a4534206
```

Figure 6: User credentials obtained from the cache using Invoke-Mimikatz.ps1.

4.2. Recommendations

Table 1 provides a brief summary of the attacks used and the recommendations made regarding the vulnerabilities observed during our scenario.

Table 1
Summary of Recommendations

Vulnerabilities	Attacks	Recommendations
1. Possibility of access to sensitive data (user privileges, software and application execution rights, etc.)	Execution of dangerous scripts and commands for vulnerability enumeration through memory evasion method	Perform regular audits to check for suspicious command executions
2. Use of software and applications with vulnerabilities	Substitution of files or executables with malicious files	- Check for software vulnerabilities before installation - Identify and prioritize monitoring of high-risk software and applications [25] - Restrict access to various folders and storage areas - Regularly verify compliance and assess security settings with each new version of hardware or software [25] - Conduct regular audits of granted permissions and privileges
3. Availability of domain user credentials in encrypted or non-encrypted form in machine caches	Credential retrieval through script execution and tools like Invoke-Mimikatz	- Prevent the use of high-privilege accounts on unauthorized systems [25] - Configure complex password policies - Limit the number of cached user credentials -Implement controls to allow temporary membership of a user in privileged groups when necessary [25]

5. Conclusion and Perspectives

This work highlighted the dangers to which domain environments are exposed in case of misconfiguration through a scenario and proposed appropriate recommendations to mitigate them. Using techniques from the MITRE ATT&CK® framework allowed for a better understanding of the variety of attack techniques. This scenario is the first of a long list of possible attack scenarios currently being implemented.

There are a large number of attack techniques on MITRE ATT&CK®. Therefore, it would be interesting to carry out other scenarios with these techniques and even other access management tools such as JumpCloud and Azure Active Directory.

References

[1] Qu'est-ce que l'infrastructure IT ?, 2023. URL: https://www.ibm.com/fr-fr/topics/infrastructure.

[2] Ö. Aslan, S. S. Aktuğ, M. Ozkan-Okay, A. A. Yilmaz, E. Akin, A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions, Electronics 12 (2023).

[3] Paysages Des Cybermenaces en Afrique en 2023, 2023. URL: https://afcsm.com/paysages-des-cybermenaces-en-afrique-en-2023/.

[4] Gestion des accès Active Directory, https://www.isdecisions.fr/gestion-acces-active-directory/, 2022.

[5] B. I. Mokhtar, A. D. Jurcut, M. S. ElSayed, M. A. Azer, Active directory attacks—steps, types, and signatures, Electronics 11 (2022). URL: https://www.mdpi.com/2079-9292/11/16/2629. doi:10.3390/electronics11162629.

[6] A. B. Ajmal, M. A. Shah, C. Maple, M. N. Asghar, S. U. Islam, Offensive security: Towards proactive threat hunting via adversary emulation, IEEE Access 9 (2021). doi:10.1109/ACCESS.2021.3104260.

[7] iainfoulds, Présentation des services de domaine Active Directory, https://learn.microsoft.com/fr-fr/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview, 2023.

[8] The threat landscape | Microsoft Press Store — microsoftpressstore.com, 2019. URL: https://www.microsoftpressstore.com/articles/article.aspx?p=2992603&seqNum=2.

[9] C. Chindrus, C.-F. Caruntu, Securing the network: A red and blue cybersecurity competition case study, Information 14 (2023).

[10] CyberSecura, La norme ISO 27001 et le SMSI (Système de Management de la Sécurité de l'Information), https://medium.com/cybersecurity-and-gdpr-compliance/la-norme-iso-27001-et-le-smsi-syst%C3%A8me-de-management-de-la-s%C3%A9curit%C3%A9-de-linformation-304a1fae59dd, 2023.

[11] J. Robert, Système d'information (si): Qu'est-ce que c'est?, 2023. URL: https://datascientest.com/systeme-dinformation-tout-savoir.

[12] B. Oni, A. Kpelafiya, Windows active directory vs. linux directory services (2023).
[13] C. D. Motero, J. R. B. Higuera, J. B. Higuera, J. A. S. Montalvo, N. G. Gómez, On attacking kerberos authentication protocol in windows active directory services: A practical survey, IEEE Access 9 (2021) 109289–109319.
[14] A. Pektaş, Practical approach for securing windows environment: Attack vectors and countermeasures, International Journal of Network Security & Its Applications (IJNSA) Vol 9 (2017).
[15] MITRE ATT&CK, https://attack.mitre.org/, 2015.
[16] PowerSploit/Privesc at master · PowerShellMafia/PowerSploit, https://github.com/PowerShellMafia/PowerSploit/tree/master/Privesc, 2021.
[17] Mimikatz, https://adsecurity.org/?page_id=1821, 2018.
[18] System Information Discovery, Technique T1082 - Enterprise | MITRE ATT&CK, https://attack.mitre.org/techniques/T1082, 2017.
[19] Account Discovery, Technique T1087 - Enterprise | MITRE ATT&CK, https://attack.mitre.org/techniques/T1087, 2017.
[20] Permission Groups Discovery, Technique T1069 - Enterprise | MITRE ATT&CK, https://attack.mitre.org/techniques/T1069, 2017.
[21] Impair Defenses: Indicator Blocking, Sub-technique T1562.006 - Enterprise | MITRE ATT&CK, https://attack.mitre.org/techniques//T1562/006/, 2020.
[22] Masquerading: Match Legitimate Name or Location, Sub-technique T1036.005 - Enterprise | MITRE ATT&CK, https://attack.mitre.org/techniques/T1036/005/, 2020.
[23] Credentials from Password Stores, Technique T1555 - Enterprise | MITRE ATT&CK, https://attack.mitre.org/techniques/T1555/, 2020.
[24] Os credential dumping, technique t1003 - enterprise | MITRE ATT&CK, https://attack.mitre.org/techniques/T1003/, 2017.
[25] iainfoulds, Best Practices for Securing Active Directory, https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory, 2023.