ISSN: 2583-9888
DOI: doi.org/10.51219/JAIMLD/Srikanth-mandru/176

URF PUBLISHERS
connect with research world

Journal of Artificial Intelligence, Machine Learning and Data Science

https://urfpublishers.com/journal/artificial-intelligence

Vol: 1 & Iss: 1

Research Article

Advanced Strategies for Detecting and Responding to Active Directory Security Breaches: A Focus on Digital Forensics

Srikanth Mandru*

Citation: Mandru S. Advanced Strategies for Detecting and Responding to Active Directory Security Breaches: A Focus on Digital Forensics. *J Artif Intell Mach Learn & Data Sci 2022*, 1(1), 698-702. DOI: doi.org/10.51219/JAIMLD/Srikanth-mandru/176

Received: 02 September, 2022; **Accepted:** 18 September, 2022; **Published:** 20 September, 2022

***Corresponding author:** Srikanth Mandru, USA, E-mail: Mandrusrikanth9@gmail.com

ABSTRACT

AD security or Active Directory security is essential because it is one of the pillars of the IT infrastructure and is vulnerable to sophisticated threats. The approaches that can be used to counter AD breaches, such as threat detection through AI, honeypots, anomaly detection, and continuous monitoring, have been explained in this article. To state the sources of threats and enhance AD security with the assistance of a background study on the role of digital Forensics. Some areas within implementing these are digital Forensics, prevention, and continuous improvements, which are vital if organizations are to survive, as well as sound detection and response strategies.

Keywords: Active Directory (AD), Security Breaches, Digital Forensics, Intrusion Detection, Incident Response, Forensic Analysis

1. Introduction

A company's network's Microsoft Active Directory architecture is safeguarded by cybersecurity methods and practices known as Active Directory (AD) security. Given that compromising AD may lead to immense levels of access and control of the network, it plays a vital role and thus makes it a desirable target for cyber extortion, as shown in **(Figure 1).** The mix of activities, including credential harvesting, the elevation of privilege, and network movements, has made it easier for threat actors to target AD in the threat landscape[1]. The future actions that should have been should have been done other than NotPetya and SolarWinds are still in the experimental stage.

To minimize threats, proven detection techniques and action plans are needed. Information means postferent continuous observation, deviation assessment, and event-related decisive reaction to quickly identify and respond to the harmful activity. However, if what was mentioned above does not sufficiently address the issue, one must use something more substantial. Digital Forensics encompasses several methodologies, gadgets, and models necessary for the identification, acquisition, and examination of digital evidence crucial for AD's security. The assessment describes the danger and the vulnerability so that the IT administrators can see where and when the hack occurs. Such information helps improve the protection of AD security, a more proactive approach when they are informed, and better reaction methods in general. But, to construct a contextually relevant and secure AD IT environment, it is imperative to determine what digital Forensics is and where the security sphere.

2. Problem Statement

The main attribute of AD is that it is embedded and serves as an internal IT structure in many firms, making it a favorite to attackers. Among the problem areas in AD design that may lead to attackers are harmful monitoring of old software and the wrong permission level[2]. In such cases, they include credentials

theft, privilege elevation, and traversal across the targeted system.

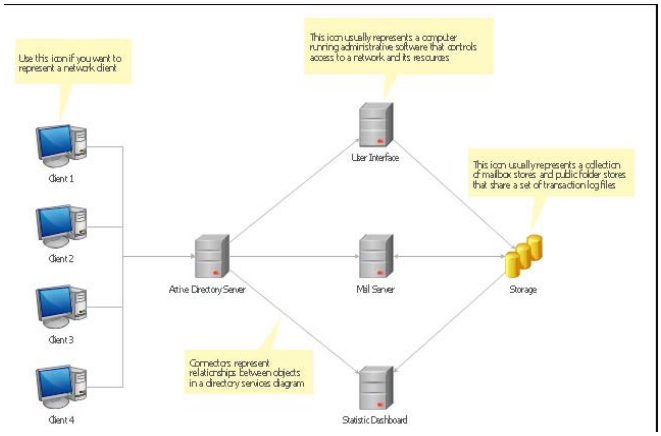

Figure 1: Active Directory structure diagram[1].

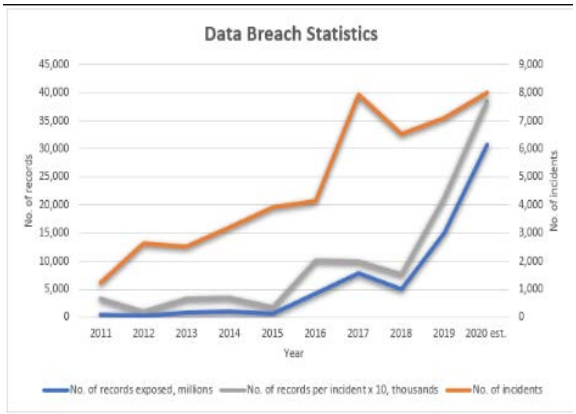

Figure 2: Increase in AD Breaches[2].

One of these is to phish the credential account and then utilize this to gain illegitimate access. Then, she escalated using the Kerberos ticket-granting ticket or TGT. Mimikatz, coupled with such programs, reads through the contents of memory and extracts items such as Kerberos tickets and other plaintext passwords, which the attacker can use to move around a network unobserved. More documented and highly profiled attacks have made all these weaknesses public[3]. As seen in the case of the SolarWinds attack, it helped them to undermine proper structures and move within the structures and systems. Likewise, the NotPetya ransomware could comment on all business systems quickly due to the lack of adequate AD configuration settings, resulting in downtimes and millions of dollars lost.

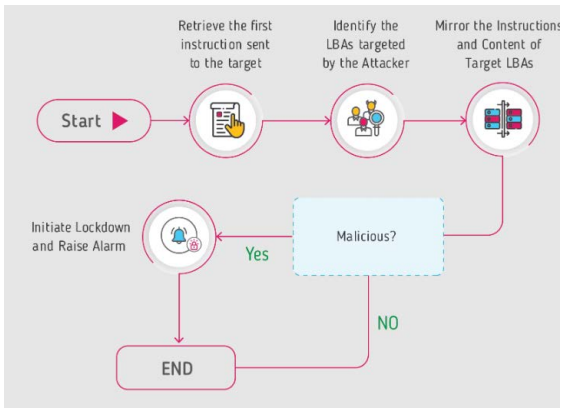

Figure 3: The NotPetya attack process[4].

The following cases serve as an installment of the more nuanced methods attackers use to launch their malware and exploit AD vulnerabilities.

Understanding the following factors is necessary to comprehend why it's challenging to identify and respond to AD breaches. However, it should be noted that typical indications of penetration, such as special login times or account usage, are not discernable using conventional security measures[4].

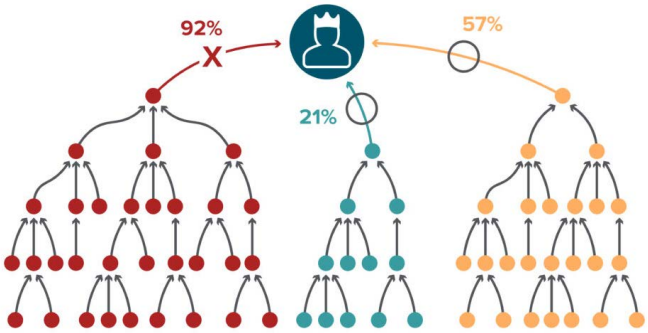

Figure 4: Common Attack Vectors in Active Directory

Attackers often use other tactics to remain unseen, such as wiping system event logs and spoofing real system administrator applications, as shown in **(Figure 5)**. Sometimes, for example, excellent anomaly detection systems or other complicated monitoring systems do not exist.

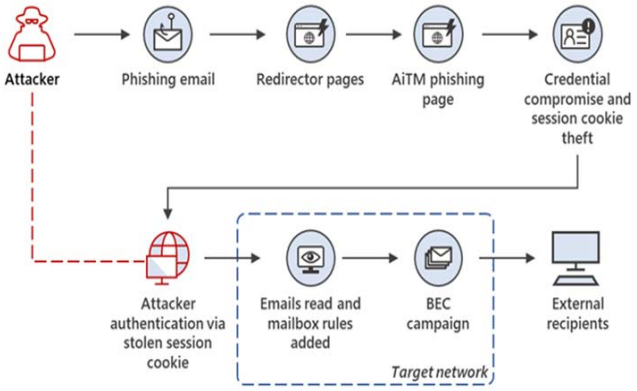

Figure 5: Phishing Attack Process Active Directory[5].

This presents many difficulties for the responders because the process of dousing the disaster is always fast and has more complications. However, it is essential to note that responding quickly and effectively, whenever possible, is problematic because of often intricate AD settings and because not all relevant data are easily discernible. It gets worse when other IT and security groups participate in all the evidence events and make sure preparations commence during the trivial occurrence of an event.

3. Solution

3.1. Continuous monitoring and anomaly detection

Real-time monitoring forms another core factor that lies at the heart of the process of suspicious activity identification in the Active Directory (AD). A SIEM system can help analyze real-time alerts from applications and equipment within a network. SIE systems can pick up possible security threats that may point to a security breach since these systems can incorporate real-time tracking to monitor user activities, access patterns, and operational changes[6]. Fostering this process further, the anomaly detection algorithms can also point to any miscellaneous events, for example, the logons, privilege elevation, or access that does not conform to the norm. These measures are helpful at the screening stage, thus allowing faster rates of response.

3.2. Implementation of honeypots and decoys

Using honeypots and decoys constitutes one of the practical approaches that can be applied to detect and further analyze the attack attempts within the context of the AD system. The idea of a honeypot is to lure those who want to intrude intentionally with weak replicas of structures to cease them from attacking constructive structures. In the same way, fake targets redirect attackers into announcing their position and strategy, decoys resemble valid AD objects, such as user accounts and service principals.

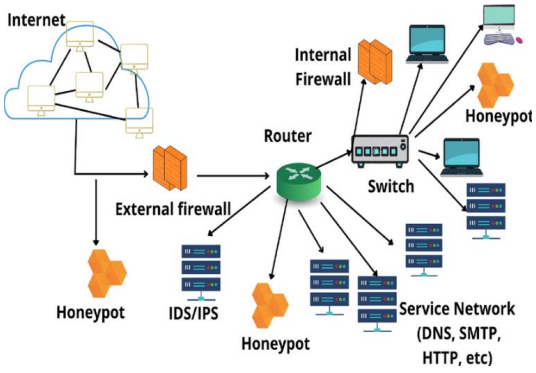

Figure 6: Honeypot system in Detecting AD Breaches[7].

One could argue that the security teams might best watch these false features to get a feel for how the owners of such kits sharpen their defenses and gain invaluable knowledge about the various tricks they pull. Exploring the Potential of AI and Machine Learning for Threat Detection

Likewise, AD settings are made using machine learning (ML) and artificial intelligence as potential means of threat recognition. They can go through layers of information to seek out patterns and outliers that could be missed through other conventional methods. Another program can educate ML on how to search for indicators of compromise (IOCs) and future attack patterns using attack data that has got there[8]. This way, the information collected from different sources can be integrated, and AI may enhance this process and result in an overall view of the security threats. By so doing, intelligent threat detection to the AD security measures should also be enhanced, and the outcome should be improved when integrated into the ML and the AI.

1. Effective Response Techniques to AD Breaches

3.3. Incident Response Planning and Execution

Some measures that can be put in place when it comes to managing AD breaches include: For an organization to deal with AD breaches, it is necessary to have an incident response (IR) plan in place. Elements that should be encompassed in this strategy are GED, safety evaluation, and security response. Such measures include constituting an IR team, visonizing responsibilities, and creating communication structures [8]. Hiring a dedicated IR team is not enough; the IR team needs to be trained and engage in practice sessions more often to be aptly prepared in the event of actual crises. Implementing an IR strategy faster may reduce the consequences and time taken to resolve the issue.

2. Containment, Eradication, and Recovery Processes

In the case of an AD breach, it becomes essential to respond to the threat immediately to tone the uncovering of the assault. In this process, accounts that will be compromised must be temporarily locked, and the IP addresses most likely to be owned by a malicious user or an attacker must be banned.

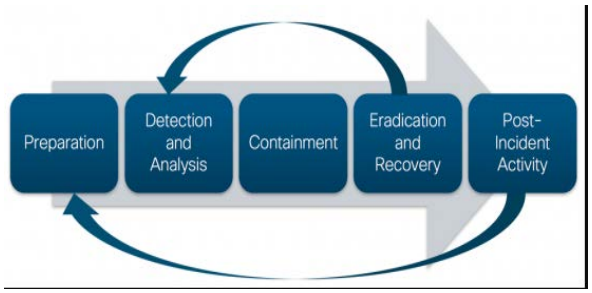

Figure 7: Dissecting a Breach[9].

The systems affected by this type of attack must be quarantined. The second process is cleaning or removing the offending malware or backdoors that led to the incursion in the first place from the affected systems. The main objectives that can be set for the recovery procedures are to return the affected systems to a regular functioning state, identify vulnerabilities and threats that might have been exploited in the attack, and monitor for signs of continued adversary presence. For better results in the future, it is essential to state the actual occurrence and the actions taken to address it.

3.4. Role of automation in response efforts

However, in the sense of effectiveness and efficiency of incident response activities, automation is needed for data, identification of an irregularity, and the introduction of specific remedial actions such as isolating the computers affected or revocation their right of access are some of the capabilities of the automated type[10]. The following are some of the benefits of automation in handling security personnel. Automation has allowed security personnel to minimize time spent on mundane tasks, focusing their time and efforts on meaningful projects, including long-term planning. Furthermore, the short-term loss from an AD breach might be less due to the use of artificial intelligence in identifying and responding to such violations in real time, eliminating the time it takes to notice the problem and work on the solution.

4. Uses

4.1. Collection and Preservation of Digital Evidence

Another exciting reason is that digital Forensics plays a vital role in detecting AD intrusions as it presupposes gathering digital information that may be useful in investigations. This would ensure that the evidence cannot be altered in some ways since it is well understood that in any cyber attack, screenshots of the affected PCs and system event logs, besides capture of the flow of the network traffic, would be taken. Legal procedures on civil and corporate matters, investigative activities, and management of evidence also demand that evidence can only be supposed to have been kept under chain-of-custody rules[10]. If any of these sources or the mechanism of AD breaches is known, it can be identified with the help of the mentioned instruments of forensic investigation. Other methods used by the investigators in the identification process include timeline analysis, data carving, and malware reverse engineering to understand what led to the attack.

Since forensic data may contain valuable information, computer forensic experts are likely to know not only the location of the break but how it happened within the network or the portion accessed. For those who wish not to experience such

a type of attack in the future, one needs to analyze this event to conclude.

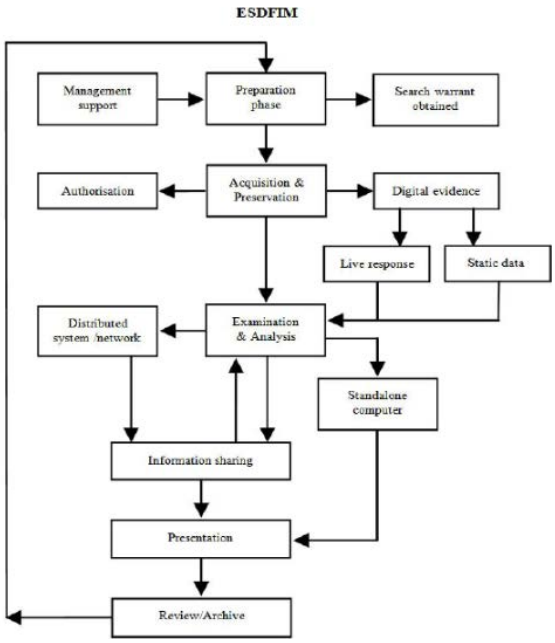

Figure 8: Digital Forensic Analysis Process[11].

4.2. Use of forensic tools and software in ad investigations

To increase the effectiveness and specificity of the forensic process within the investigation of AD cases, the organizations employ several tools and methods. Different tools, such as Wireshark, EnCase, and FTK (Forensic Toolkit), are used to analyze the electronic evidence to do this. Further, other unique AD forensic tools that can be employed to examine the AD design and search for configuration problems and threats- like DS Internals and Bloodhound[12]. With these resources, forensic specialists might conduct investigations that are more accurate and done more quickly.

Figure 9: Tools used in digital Forensics[12].

4.3. Successful detection and response using digital forensics

One of the most notable examples of a forensic investigation of a large international financial institution was a highly severe AD breach in 2018. FREM analysis helped establish that the attackers initially got into the system through a zero-day exploit and then got elevated privileges and transmitted high-value data through APIs[12]. A case that played out in 2021 illustrated just how helpful digital Forensics can be in detecting and halting a ransomware attack on a hospital. The incident was traced back to originating from a phishing email, and investigators could also track the lateral movement of the AD and solve the encryption without paying for the ransom.

5. Impact

AD security makes an organization's security much better by putting many procedures in place to detect or even respond to various intrusions to AD. These tactics are also good at keeping attackers' footprints within the system for shorter times as their presence is detected more often. Incident response skills that are built reduce the likelihood that an organization will experience considerable loss of data or operations since threats are effectively addressed and averted. Additionally, employing both digital and digital Forensics helps establish complex investigations that encompass information that may be useful in preventing such attacks in the future. Measures for AD security prevention are anticipated investments that are capitalized beforehand. Other activities are post-scan monitoring, threat identification with the assistance of AI technologies, and other forms of automatic response[13].

On the other hand, the investments from these resources could yield great long-term cost benefits if the practices established are efficient. Possible penalties for one severe offense often may be much higher than Castile safeguards, not to mention legal costs, penalties, tarnished reputation, and sales. Furthermore, anticipatory security cancels long periods of being out of order and ensures the survivability of companies and their organizations; it contributes to building greater confidence in clients and achieving better results.

Organizations that embrace these advanced detection and response strategies will fortify their security stance over time. Security measures are frequently changed and enhanced so that the latest security standards protect the company.

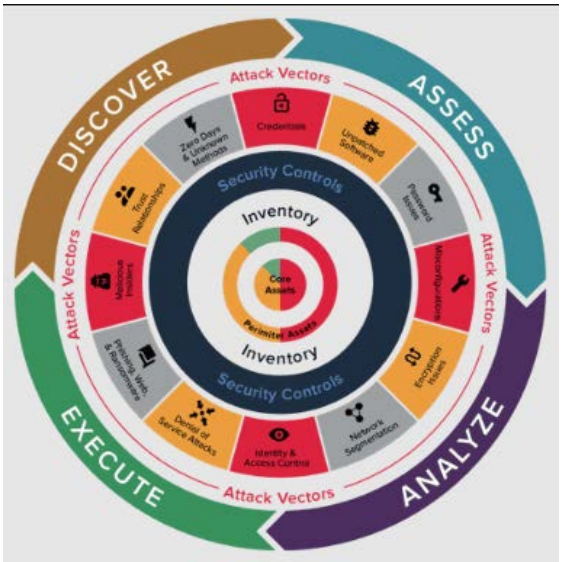

Figure 10: Implications of AD security for Organizational Security Posture[14].

Enhanced forensic capability helps in learning from such occurrences and cultivating a constant improvement perspective[14]. Besides providing instantaneous protection against threats, it makes the business culturally safe and ready to reduce risks inherent in operations in the long run.

6. Scope

Certain imperatives and challenges are involved when it comes to the use of complex detection and response procedures of AD security. The use of artificial intelligence for threat identification and constant monitoring and protection requires relatively large expenditure; moreover, it is essential to address expert knowledge, which not every enterprise is equipped with. Third, there are integration issues because implementing the new security solutions may be complicated with the current system architecture[15]. There is also a challenge of engaging IT and security professionals to upgrade their understanding of these cyber threats as they evolve rapidly.

Going further, AI automation will likely be used to handle future attacks. As the technique of machine learning improves, the possibility of detecting more advanced attack signatures will become possible. Another dawning notion is called Zero Trust Architecture (ZTA). This architectural model embraces the tenet of 'never trust, always check 'to minimize the chances of an intrusion. Technological trends of extensive data analysis and cloud forensics have improved the effectiveness of digital forensic investigation, thus resulting in increased overarching intricate attack analysis. Further investigation is required to integrate AI into conventional security frameworks better and develop enhanced anomaly detection frameworks.

Similarly, more studies on the other applications of blockchain technology, such as the secure login and storage of proofs in Forensics, are also required. ''Enhancing the security of the AD environment also involves the people or actors in a system, especially the users and their degree of awareness and cybersecurity training. What shall then be of paramount importance in AD environments is that standards must be followed by the forensic and the incident orders, which shall align with the security objectives.

7. Conclusion

This research pointed out the critical vulnerabilities in AD and the exact methods used in attacking these vulnerabilities. The study has explored the intricate detection and response strategies, always emphasizing the need to monitor continuously, use artificial intelligence in threat identification, use honeypots, and implement effective incident handling strategies. Since the goal is to enhance the security of AD, then one has to employ digital Forensics that gives deep insights into the attack to avoid future occurrences. Ensuring such a security position requires enhancing such strategies, which can only be achieved over time. Considering the level of AD security and being ready for further forensic examination is essential for preventing companies from additional loss of computing resources and having an ultimate defense against cyber threats as a permanent solution.

8. References

1. McDonald G, Papadopoulos P, Pitropakis N, Ahmad J, Buchanan WJ. Ransomware: Analysing the impact on windows active directory domain services. Sensors 2022;22: 953.
2. Ebad SA. Lessons learned from offline assessment of security-critical systems: The case of microsoft's active directory. Int J Sys Assurance Engineering Management 2021;13: 535-545.
3. Montero CD, Higuera JRB, Higuera JB, Montalvo JAS, Gomez NG. On attacking kerberos authentication protocol in windows active directory services: A practical survey. IEEE Access 2021;9: 109289-109319.
4. Srinivasa S, Pedersen JM, Vasilomanolakis E. Deceptive directories and 'vulnerable' logs: a honeypot study of the LDAP and log4j attack landscape. 2022 IEEE European Symposium on Security and Privacy Workshops 2022.
5. Chatterjee A, Ahmed BS. IoT anomaly detection methods and applications: A survey. Internet of Things 2022;19: 100568.
6. Amma BNG, Selvakumar S. Anomaly detection framework for Internet of things traffic using vector convolutional deep learning approach in fog environment. Future Generation Computer Systems 2020;113: 255-265.
7. Feng F, Liu X, Yong B, Zhou R, Zhou Q. Anomaly detection in ad-hoc networks based on deep learning model: A plug and play device. Ad Hoc Networks 2019;84: 82-89.
8. Aggarwal P, Du Y, Singh K, Gonzalez C. Decoys in Cybersecurity: An exploratory study to test the effectiveness of 2-sided deception. arXiv 2021.
9. Sun B, Ban T, Han C, et al. Leveraging machine learning techniques to identify deceptive decoy documents associated with targeted email attacks. IEEE Access 2021;9: 87962-87971.
10. Mohanta BK, Jena D, Satapathy U, Patnaik S. Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology. Internet of Things 2020;11: 100227.
11. Liu Q, Li P, Zhao W, Cai W, Yu S, Leung VCM. A Survey on security threats and defensive techniques of machine learning: A data driven view. IEEE Access 2018;6: 12103-12117.
12. Awuson-David K, Al-Hadhrami T, Alazab M, Shah N, Shalaginov A. BCFL logging: An approach to acquire and preserve admissible digital forensics evidence in cloud ecosystem. Future Generation Computer Systems 2021;122: 1-13.
13. Piedrahita AFM, Gaur V, Giraldo J, Cardenas AA, Rueda SJ. Leveraging software-defined networking for incident response in industrial control systems. IEEE Software 2018;35: 44-50.
14. González-Granadillo G, González-Zarzosa S, Diaz R. Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. Sensors 2021;21: 4759.
15. Ashraf J, Moustafa N, Khurshid H, Debie E, Haider W, Wahab A. A review of intrusion detection systems using machine and deep learning in internet of things: Challenges, solutions and future directions. Electronics 2020;9: 1177.