LDAP and Log4J attacks

Abhishek Verma
Dept. of Computer Science
New York University
NY, USA
av2783@nyu.edu

***Abstract*—Directory services can be queried with the Lightweight Directory Access Protocol (LDAP). Most commonly, it is used to read, write, and search directory services, such as Active Directory. Many attacks have been attempted using LDAP authentication as a result of its widespread adoption, including injection attacks and unauthorized access due to third-party key storage. A recent vulnerability discovered in Log4j can enable adversaries to obtain unauthorized data from directory services through pivoting attacks. In addition, LDAP can be configured to operate over UDP, allowing adversaries to exploit it for Distributed Reflection Denial of Service (DRDoS). A study is presented in this paper on attacks on LDAP by way of honeypots that simulate multiple profiles of the service. In a period of one month, 39,388 malicious events were observed, targeting honeypots and 273 unique attack sources performing pivot attacks.**

I. Introduction

Directory services have been queried and searched using LDAP (Lightweight Directory Access Protocol) for many years. LDAP is the lightweight implementation of the Directory Assistance Service (DAS) of the X.500 protocol (also known as Directory Access Protocol) [1], [2]. LDAP's lightweight implementation enables many applications to synchronize and manage directory services (e.g., Microsoft's Active Directory Server). Users, applications, computers, and devices in the network can query LDAP directory services for attributes via an LDAP client [3]. A range of enterprise applications use LDAP for authentication, including email clients, SSH, servers, and workstations.

Over the years, LDAP has been vulnerable to a variety of attacks including injection attacks, unauthorized access, and remote code execution [4]– [6]. Due to the widespread use of LDAP in enterprise applications, attackers are highly motivated to exploit the protocol to gain unauthorized access to targeted infrastructures. In 2020, several DDoS campaigns used UDP-based LDAP services, according to the ENISA Threat Landscape Report 2021. The DNS and LDAP services were efficiently used to amplify DDoS attacks on French, Belgian, and Dutch Internet Service Providers [7]. In addition, Project Sonar [8] discovered that up to three million LDAP servers appeared on the Internet with open TCP port 389, accepting unencrypted requests. This suggests that poorly configured LDAP servers can cause significant harm.

A honeypot is a system or service that replicates the target system or service. By acting as decoys, they attract attacks and store all attack traffic. Honeypots are traditionally used to gather data on bot attacks and threat intelligence. Honeypots can be used to test specific protocols or vulnerabilities [9]. Some of these open-source projects are maintained by the Honeynet Project. This simulation covers a wide range of application protocols in IT, OT (Operational Technology), and IoT environments. Honeypots have been an obvious choice for studying attack trends and, more recently, about attacker behavior psychology [10].

In this paper, we study a honeypot that simulates open-source implementations of directory services to gather attack trends in LDAP. Moreover, there is a Log4j component to the honeypots to allow an analysis of pivoting attacks towards LDAP.

II. Related Work

A discussion of LDAP attack types and LDAP honeypots is presented in this section.

A. LDAP attacks

Over the years, LDAP has been reported as having several vulnerabilities. Several LDAP implementations [11] have been attacked using Denial of Service, remote code execution, and privilege escalation techniques. Moreover, the LDAP protocol was exploited as part of APTs that exploited other vulnerabilities (such as CVE-2021-44228 of the Apache Log4j vulnerability) [12]. In the early research by Alonso et al. [5], injection techniques were demonstrated using LDAP. Using the search filters for the directory service, the authors present injection techniques. Obimbo et al. demonstrate the dangers of using LDAP as an authentication protocol by executing a DoS attack exploiting the TCP three-way handshake required for connection initialization with an LDAP server [4]. More recently, Jeitner et al. described injection attacks against DNS, LDAP, and Eduroam [6] protocols using malicious payloads. In the enterprise infrastructure, LDAP is widely used for authentication, so any possible attack vector against it is high risk.

B. LDAP honeypots

Grimes proposed early work on LDAP honeypots [13]. In the article, the author discusses honeypots in general and Windows-based honeypots that administrators can use to detect potential zero-day attacks. In addition, the author provides an overview of how to model honeypots using scripts from the HoneyD honeypot framework [14]- [16]. Using the honeypot framework HoneyD, virtual hosts on a network can be created that can run arbitrary services. The daemon can operate on multiple addresses and use scripts to emulate a device or a specific protocol. Additionally, research is being conducted that proposes using Honeytokens, subsets of honeypots that replicate digital entities like user accounts, files, and folders to detect malicious activity. To capture malicious access attempts, Lukas et al. propose creating fake user accounts as honeytokens on Active Directory Server [17].

There are 25 different honeypots included in the T-Pot project [18], including the Log4Pot honeypot [19]. A vulnerable Log4J environment can be simulated by Log4Pot, which can be configured to listen on multiple ports. Honeypots also provide log analysis tools that abstract attack payloads, process them, and create timelines of the attacks. In the GreedyBear Project [20], attack data from the T-Pot project honeypots, specifically from Log4Pot and Cowrie, is aggregated and converted into actionable threat intelligence feeds. Honeynet maintains the GreedyBear project [9] and provides access to feeds aggregated by GreedyBear to the public. However, no honeypots have been developed to capture LDAP-specific attacks.

III. Methodology

The methodology for setting up and analyzing attacks from the Honeynet Project community is presented in this section, including the experimental setup and the LDAP honeypot implementation.

A. LDAP honeypot

A honeypot that can operate in hybrid-interaction levels [21] is extended to simulate the LDAP service by extending the open-source RIoTPot. In addition to the provision of high-interaction capabilities, RIOTPOT also records traffic as pcap files and in a database of attacks. Taking into account the modular nature of RIoTPot, which simplifies the integration of protocols and services into the simulation portfolio, three profiles were integrated: Apache Directory Server [22], OpenLDAP [23], and OpenDJ [24]. All three support the LDAP services and are run as containers. RIoTPot's orchestration and logging features were used to capture the attack traffic from the three profiles. Additionally, the Log4J vulnerability [12] of web-services is simulated which refers to the simulated directory services in containers via profiles. In total, three webservices were deployed that connect to individual directory services. The description of these simulated profiles is presented below.

1) Apache Directory Service: Apache Directory Server (ADS) [22] implements Directory services in an open-source, extensible manner. It is implemented using the Java programming language and can be incorporated into a server application as a module. The ADS server supports communication through LDAP Version 3 and is compatible with that protocol. Apart from LDAP, ADS also supports Kerberos 5 and Change Password. ADS also uses a subentries scheme with the X.500 basic access control scheme to control how access and attributes are handled in the Directory Information Tree (DIT). An LDIF file can be used to define the properties of DIT, directory objects, and attributes for the directory service. ADS is actively maintained by the Apache community.

2) OpenLDAP: The OpenLDAP project implements LDAP as an open-source project [23]. Packages include LDAP load-balancing, LDAP service daemons, and libraries that implement LDAP with additional utilities. LDAP connections are listened by lloadd on a specified number of ports and forwarded to the backend for processing, while LDAP requests and queries are heard by slapd. Further, slapd provides a tool mode that allows multiple profiles to be used.

3) OpenDJ: The OpenDJ directory service is an open-source LDAPv3 compliant implementation developed in Java [24]. Among the features of the implementation are scalability for large domains, monitoring tools, and replication between multiple instances. Along with LDAP v3 and Directory Service Markup Language (DSMLv2), OpenDJ supports LDAP v2. An open source project, OpenDJ is actively maintained by the OpenIdentity Platform.

4) HTTP Service with Log4j vulnerability: For debugging applications, Log4j provides multiple logging levels. It is a free open-source logging library for Java. Applications utilizing this library are widespread. According to a recent report [12], a bug in the Log4j library allows an attacker to run code remotely on a victim using the library for debugging. When a configuration uses a JNDI LDAP data source URI along with a JDBC Appender, unauthorized users are able to run arbitrary code on the target machine [25]. Log4j attacks can be carried out by attacking malicious LDAP servers. Using a honeypot setup that includes an HTTP service that showcases the Log4j vulnerability and configures them to connect to individual directory services, any potential pivot attacks that could target LDAP services via the Log4j exploit can be discovered. A login dashboard is simulated on these websites, which includes a welcome header, fields for logging in, and a login button. The login button validates the username and password from the configured directory service using a standard procedure. In order to enable the examination of LDAP injection attacks, the websites are hosted in the same instance as the directory simulations, and a search user is created with access to search the directories.

B. Experimental Setup

In order to capture attacks on individual profiles, we deploy RIoTPot on three hosts, each of which simulates a directory service and an HTTP service. As shown in Fig. 1, this lab environment is set up to test honeypots. Hosts are assigned public IP addresses and have ports 389 (LDAP) and 80 (HTTP) open to the Internet. Each host's traffic is captured in a pcap file and stored in a remote repository. In addition, all traffic received on ports 80 and 389 is logged in a database that determines whether it is an attack. To avoid disruption in logging in case of a crash, the file repository and attack database are set up on a remote host. An admin username and a non-complex password are set up for the directory service's basic authentication.

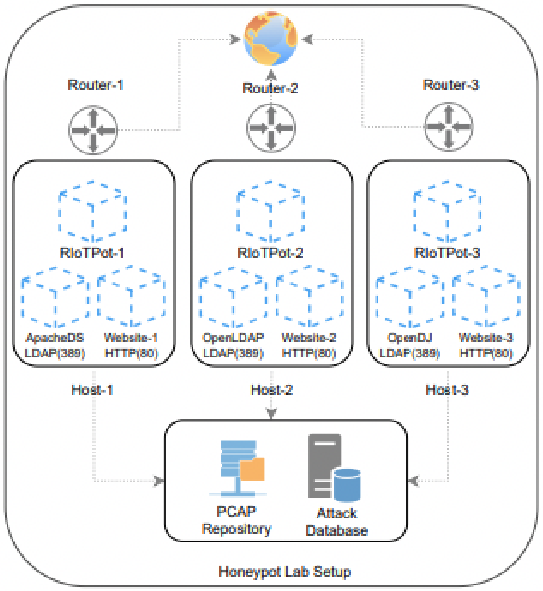


Fig. 1. Overview of the experimental setup

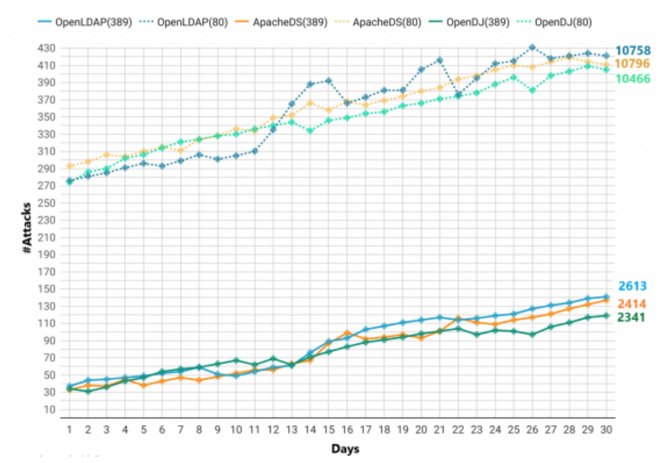


Fig. 2. Attacks received over 30 days - LDAP and HTTP

IV. Results

The findings on the attacks are listed here.

A. Attack traffic count

The traffic is classified as suspicious if it exhibits an injection pattern or an irregular search pattern [5]. If brute-force attempts are detected on HTTP, and remote code execution patterns are detected, the traffic is classified as an attack. Based on the number of attacks received on each profile over port 389 and 80 over a 30-day period, Fig. 2 summarizes the number of attacks experienced by each profile. A total of 39,388 attacks were recorded. In comparison to ApacheDS (2414) and OpenDJ (2341), OpenLDAP recorded the most LDAP attacks (2613). As the deployment progressed, attacks on all three profiles continued to increase. There is a possibility that the profiles were listed on Internet-wide scanning services. The attacks shown are exclusive of probing traffic from known Internet scanners. The HTTP service recorded a total of 22,673 events, while the LDAP service recorded 8,100 events from known scanning services. RIoTPot's noise-filter module identified the traffic from these benign scanning services.

B. Attack sources

Due to the honeypots being exposed to the Internet, Internet-wide scanning services generated a large amount of benign traffic on them. Fig. 3 below shows the distribution of traffic generated by scanning services (beneficial) and malicious attacks. The RIoTPot service (RIoTPOT) identifies the probing traffic from 19 Internet-wide scanning services [21] and filters it from the honeypots. This process reduces noise in the gathered data by filtering benign scanning traffic, allowing the suspicious traffic to be analyzed more closely. As interacting with a honeypot provides no productive value, all traffic towards honeypot instances can be considered suspicious. There were 273 unique sources of attacks on the honeypots.

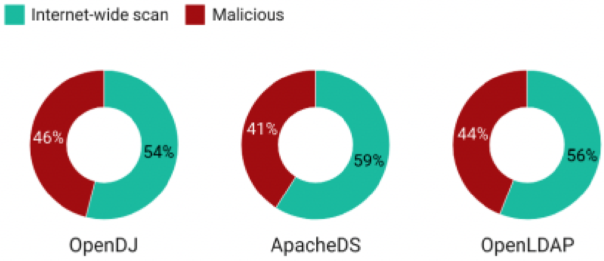


Fig. 3. Traffic classification on honeypots

C. Attack types

Fig. 4 shows each simulated directory service's attack types in percentage terms. Compared to other profiles, the OpenDJ profile received the most LDAP Injection attacks. In these attacks, the userPassword attribute was retrieved blindly by utilizing exploitation techniques to bypass authentication. Additionally, the profiles received suspicious search queries from LDAP filters involving logical operators. Additionally, many brute-force attacks were detected on the HTTP web service. Furthermore, the websites were also targeted by attacks exploiting the Log4j vulnerability. Due to the time elapsed since the disclosure of the vulnerability, Log4j experienced fewer attacks than other attack types.

V. Discussion

This section discusses the findings mentioned in the previous section along with some additional results.

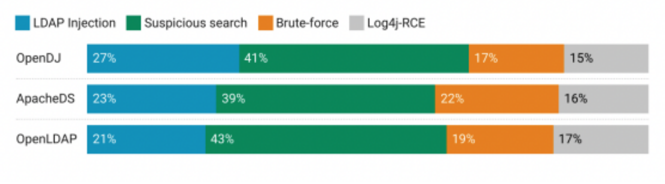
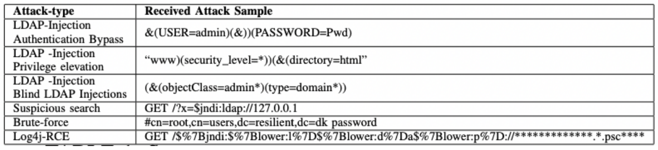


Fig. 4. Attack types received on honeypots

A. Attack samples

Examples of attacks for each attack type are shown in Fig. 5 for each category in Fig. 4. Additionally, Fig. 5 displays various LDAP injection attacks observed on the honeypots. With an Authentication Bypass attack, filtered LDAP queries are injected with sequences that bypass authentication. By exploiting the low-security search sequence, privilege escalation attacks list unauthorized directory contents. There were reports of unauthenticated injection attacks that asked for a Boolean operation to check if a domain type contains a class in the admin section. A great number of suspicious search queries were received by the honeypots. For example, the sample in Fig. 5 requested a sequence from the same host's LDAP service. Essentially, the adversary performed reconnaissance to discover open LDAP ports on the host before performing this search. Several brute force attacks were spotted in which adversaries tried to log in with a list of passwords. According to the word list order, the passwords used were from the NMap default password list [26]. Additionally, there were Log4j attacks that performed RMI calls. Fig. 5 shows examples of Log4j exploits as well.



Attack-type	Received Attack Sample
LDAP-Injection Authentication Bypass	&(USER=admin)(&))(PASSWORD=Pwd)
LDAP -Injection Privilege elevation	"www)(security_level=*))(&(directory=html"
LDAP -Injection Blind LDAP Injections	(&(objectClass=admin*)(type=domain*))
Suspicious search	GET /?x=$jndi:ldap://127.0.0.1
Brute-force	#cn=root,cn=users,dc=resilient,dc=dk password
Log4j-RCE	GET /$%7Bjndi:$%7Blower:l%7D$%7Blower:d%7Da$%7Blower:p%7D://************.*.psc****

Fig. 5. Samples of attacks received on Honeypots

B. Pivot attacks

In a pivoting attack, the attacker moves from one compromised system to another in the same infrastructure or remotely. A few of the attacks use LDAP injection techniques to exploit the vulnerability in Log4j to pivot into the directory services. An RMI call specified through JNDI found LDAP filters listing business units, enumerating domain users, and listing domain administrators. These attacks were observed in all three simulation profiles. A pivoting attack was observed on every simulation profile, as illustrated in Fig. 6. The attacks begin with a vulnerability in Log4j, then target simulated directory services using LDAP. The analysis of 429 unique attack sources (observed exclusively on Log4j) found that 273 attempted pivot attacks on directory services.

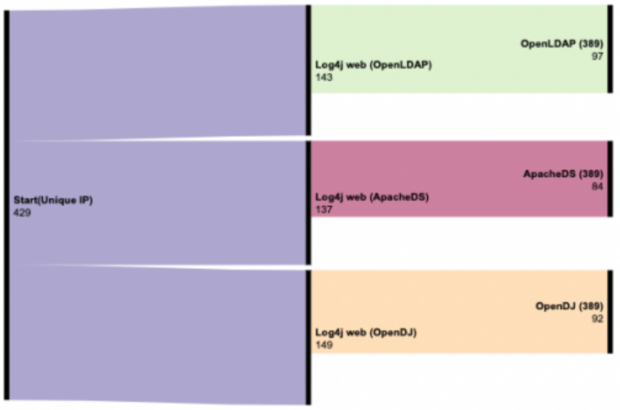


Fig. 6. Pivot attacks overview

C. Limitations

The experiments conducted had some limitations. First, only open-source LDAP and directory services implementations are considered. As most enterprises use Microsoft Active Directory as their directory service [27], this has a limited scope. Second, the experiment is limited in terms of domain simulation due to using an unregistered domain, despite simulating a high interaction profile for directory services and LDAP. A registered domain could enhance the deception layer in the experiment and appear more appealing to adversaries. Furthermore, the number of attacks observed on each profile is based only on data collected over a period of one month; a more comprehensive study is needed to provide a more holistic view of the area.

VI. Conclusion

Analyzing the attacks on LDAP using a honeypot study in this paper provides an in-depth examination. An array of attack types was observed, including LDAP injection attacks and suspicious queries. Lastly, the types of attacks are summarized.

References

[1] M. Rose,"Directory assistance service," in RFC 1202, Performance Systems International, Inc. Citeseer, 1991.

[2] B. Smetaniuk,"Distributed operation of the x. 500 directory,"Computer Networks and ISDN Systems, vol. 21, no. 1, pp. 17–40, 1991.

[3] M. Wahl, T. Howes, and S. Kille, "Rfc2251: Lightweight directory access protocol (v3)," 1997.

[4] C. Obimbo, B. Ferriman et al.,"Vulnerabilities of ldap as an authentication service." J. Information Security, vol. 2, no. 4, pp.151–157, 2011.

[5] J. M. Alonso, R. Bordon, M. Beltran, and A. Guzman, "Ldap injection techniques," in 11th IEEE Singapore International Conference on Communication Systems. IEEE, 2008, pp. 980–986.

[6] P. Jeitner and H. Shulman, "Injection attacks reloaded: Tunnelling malicious payloads over dns," in 30th USENIX Security Symposium (USENIX Security 21), 2021, pp. 3165–3182.

[7] A. Claudio, C. Stephen, S. Andreas, and D. Christos. (2021) Enisa threat landscape report 2021. [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021/@@download/fullReport

[8] Rapid7, "Project sonar," 2021. [Online]. Available: https://opendata.rapid7.com/sonar.tcp/2021-12-01-1638342851-tcp_ldap_389.csv.gz

[9] T. H. Project. (2021) The honeynet project. [Online]. Available: https://www.honeynet.org/

[10] K. J. Ferguson-Walter, M. M. Major, C. K. Johnson, and D. H. Muhleman, "Examining the efficacy of decoy-based and psychological cyber deception, in 30th USENIX Security Symposium (USENIX Security 21), 2021, pp. 1127–1144.

[11] MITRE. (2021) Ldap vulnerabilities and disclosures. [Online]. Available: https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=ldap

[12] A. S. Foundation. (2021) Cve-2021-44228. [Online]. Available: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-23302

[13] Springer, Ed., Windows Honeypot Modeling. Berkeley, CA: Apress, 2005, pp. 63–88. [Online]. Available: https://doi.org/10.1007/978-1-4302-0007-9 3

[14] N. Provos, "Honeyd-a virtual honeypot daemon," in 10th DFNCERT Workshop, Hamburg, Germany, vol. 2, 2003, p. 4.

[15] N. Provos and T. Holz, Virtual honeypots: from botnet tracking to intrusion detection. Pearson Education, 2007.

[16] N. Provos et al., "A virtual honeypot framework." in USENIX Security Symposium, vol. 173, no. 2004, 2004, pp. 1–14.

[17] O. Lukas and S. Garcia, "Deep generative models to extend active directory graphs with honeypot users," arXiv preprint arXiv:2109.06180, 2021.

[18] T. Security, "T-pot - the all in one honeypot platform," 2022. [Online]. Available: https://github.com/telekom-security/tpotce

[19] P. Thomas, "A honeypot for the log4shell vulnerability (cve2021-44228)," 2022. [Online]. Available: https://github.com/thomaspatzke/Log4Pot

[20] (2022) Greedybear honeypot feed. Honeynet Project. [Online]. Available: https://github.com/honeynet/GreedyBear

[21] S. Srinivasa, J. M. Pedersen, and E. Vasilomanolakis, "Riotpot: a modular hybrid-interaction iot/ot honeypot," in 26th European Symposium on Research in Computer Security (ESORICS) 2021. Springer, 2021.

[22] Apache. (2021) Apache directory. [Online]. Available: https://directory.apache.org/apacheds/

[23] O. Kuzn´ık. (2021) Openldap. [Online]. Available: https://www.openldap.org/

[24] OpenIdentityPlatform. (2021) Opendj. [Online]. Available: https://www.openidentityplatform.org/opendj

[25] (2021) Cve-2021-44832. Apache Software Foundation. [Online]. Available: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44832

[26] G. Lyon, "Nmap network mapper," 2021. [Online]. Available: https://nmap.org/

[27] S. Reimer and M. Mulcare, Active Directory for Microsoft Windows Server 2003 Technical Reference. O'Reilly Media, Inc, 2009.