Mini-Project 15: Network-based Cybersecurity Incident

What is CLDAP and what is it normally used for?

CLDAP, a Connection-less Lightweight Directory Access Protocol, is a UDP-based directory lookup protocol complementing the TCP-based LDAP protocol. It is a computer networking protocol designed to provide access, for querying and modifying stored data, to X.500 directory systems (Baker, 2006). CLDAP is designed to reduce the connection overheads at retrieving organizational resource information from a directory service database when using LDAP. Lightweight Directory Access Protocol (LDAP) allows remote users to look up directory data. An LDAP Directory usually contains information about users, but may also contain data about printers, servers, conference rooms, other equipment, etc. LDAP is the protocol used to access the proprietary Microsoft Active Directory (Skyway West, n.d.).

What are the two primary benefits to threat actors of amplification attacks?

The two primary benefits to threat actors of amplification attacks are:

1. Amplification of the attacker's payload could generate 5x, 10x, or 100x the traffic from their requests. To understand amplification, we need to understand the reflective distributed denial of service attacks (RDDoS). RDDoS is when a bad actor fakes the identity of the victim and requests responses for legitimate services who become unwitting accomplices. These responses overwhelm the victim's computer. It is called amplification because the bad actor only needs to send a small command to the accomplices resulting in a large amount of traffic being sent back to the victim.
2. They can spoof to hide the attacker's tracks while targeting the payloads at a specific target of their choice.

What are the five DDOS weapons that are even more prevalent than CLDAP?

The 5 prevalent DDOS weapons are:

1. Portmap: The portmap daemon helps clients map program number and version number pairs to the port number of a server.
2. SNMP: Simple Network Management Protocol (SNMP) is a networking protocol used for the management and monitoring of network-connected devices in Internet Protocol networks (IBM Documentation, n.d.).
3. SSDP: Simple Service Discovery Protocol (SSDP) is used to discover what devices (and their capabilities) are available in a local area network.
4. DNS Resolver: A DNS resolver, also called a recursive resolver, is a server designed to receive DNS queries from web browsers and other applications. The resolver receives a hostname - for example, www.example.com - and is responsible for tracking down the IP address for that hostname. (NS1, n.d.)
5. TFTP: Trivial File Transfer Protocol (TFTP) is a simple protocol that provides basic file transfer functions with no user authentication (IBM Documentation, n.d.).

What is meant by a "zero trust model?"

Organizations should not automatically trust anything inside or outside the network perimeter. Anything trying to connect to the network must be verified prior to being granted access.

How can enterprises protect themselves from these kinds of attacks?
Since the reflected CLDAP packets all come with UDP port 389 as the UDP source port, blocking or rate-limiting port 389 traffic from the internet is an effective DDoS protection method to mitigate the CLDAP reflection and amplification attack, especially if it is not expected to receive CLDAP responses from the internet. Alternatively, TCP or encrypted LDAP configurations can be used.

References

Baker, S. (2006, December 27). *Talk: Lightweight Directory Access Protocol*. Wikipedia. Retrieved February 10, 2023, from https://en.wikipedia.org/wiki/Talk%3ALightweight_Directory_Access_Protocol

IBM Documentation. (n.d.). *Search in IBM Documentation*. IBM. Retrieved February 10, 2023, from https://www.ibm.com/docs/en

NS1. (n.d.). *What is DNS? DNS Explained*. NS1. Retrieved February 10, 2023, from https://ns1.com/resources/what-is-dns

Skyway West. (n.d.). *What is a Connectionless LDAP Service Vulnerability, what is the risk and how can you mitigate that risk?* Skyway West. Retrieved February 10, 2023, from https://www.skywaywest.com/2021/07/what-is-a-connectionless-ldap-service-vulnerability/