

Forum:[Hack Forums](#)

Thread: [Retrieving Credentials from LDAP Servers in SSH Access](#)

okaaaalm - December 8, 2024, 6:05 am

Hi,

I successfully gained access to a system via SSH as a regular user. During my reconnaissance, I discovered that user credentials are stored in LDAP servers, both inside the network and externally. I have identified two IP addresses linked to these LDAP servers, but I am unable to retrieve or access the stored data.

I attempted to query the LDAP servers using ldapsearch, but it seems I require additional credentials or configuration details to proceed further.

could someone help ?

DramaKing - December 8, 2024, 7:02 am

(Dec 8, 2024 07:05 AM)okaaaalm Wrote: [\[CITE\]](#) Hi,

I successfully gained access to a system via SSH as a regular user. During my reconnaissance, I discovered that user credentials are stored in LDAP servers, both inside the network and externally. I have identified two IP addresses linked to these LDAP servers, but I am unable to retrieve or access the stored data.

I attempted to query the LDAP servers using ldapsearch, but it seems I require additional credentials or configuration details to proceed further.

could someone help ?

Use an exploit? You know that there's a Pentesting and Forensics forum, right? This isn't exactly a beginner thread.

okaaaalm - December 8, 2024, 7:33 am

Hey,

Ah, I see! I changed my account recently, which is probably why you didn't recognize me. But I've been asking around here for a while and getting great responses from you, and honestly, I've learned so much in the process. I feel much more enlightened now, and it's been really rewarding to see the progress I've made!

I didn't realize there were dedicated Pentesting and Forensics forums—thanks for pointing me in the right direction! I'm definitely eager to dive into them and learn even more.

Could you let me know where to find these forums? I'd really appreciate it!

Thanks again for all the help!

DramaKing - December 8, 2024, 4:15 pm

(Dec 8, 2024 08:33 AM)okaaaalm Wrote: [\[CITE\]](#) Hey,

Ah, I see! I changed my account recently, which is probably why you didn't recognize me. But I've been asking around here for a while and getting great responses from you, and honestly, I've learned so much in the process. I feel much more enlightened now, and it's been really rewarding to see the progress I've made!

I didn't realize there were dedicated Pentesting and Forensics forums—thanks for pointing me in the right direction! I'm definitely eager to dive into them and learn even more.

Could you let me know where to find these forums? I'd really appreciate it!

Thanks again for all the help!

Try Advanced Hacking. :P

(Dec 8, 2024 08:34 AM)m0hx Wrote: [CITE](#) im not sure but does Mimikatz help in dis kinda stuff :/? You need Domain Admin creds for a DCSync. If it's OpenLDAP (which is almost non-existent), I have no idea.

ZeroXploit - December 13, 2024, 2:30 am

access involves understanding how authentication and directory services integrate. Below is an explanation of how such systems work and ethical approaches for testing their security.

LDAP and SSH Authentication Integration

LDAP Role in Authentication:

LDAP servers store user credentials, group memberships, and other directory information.

Organizations often integrate LDAP with services like SSH to centralize authentication.

PAM (Pluggable Authentication Modules):

Linux systems commonly use PAM to integrate SSH with LDAP.

Authentication requests from SSH are passed to LDAP via PAM.

SSSD (System Security Services Daemon):

Provides access to local and remote identity and authentication resources, including LDAP.

Often used in enterprise setups to cache credentials and improve login performance.

Credential Retrieval Methods

Retrieving credentials is a sensitive topic, and the methods below are for ethical purposes like penetration testing or securing a system. Unauthorized access is illegal.

Testing LDAP Access:

Use tools like `ldapsearch` to query the LDAP directory for user data:

```
ldapsearch -x -H ldap://<ldap_server> -D "<bind_dn>" -w <password> -b "<search_base>"
```

Ensure you have legitimate credentials and permissions for testing.

Enumerating Users:

If the LDAP server allows anonymous binds, use `ldapsearch` to enumerate users:

```
ldapsearch -x -LLL -H ldap://<ldap_server> -b "<search_base>" "(objectClass=person)"
```

Sniffing Network Traffic:

If LDAP traffic is unencrypted (LDAP over TCP 389), use tools like Wireshark to capture packets and extract information. However, modern systems often use LDAPS (LDAP over SSL/TLS).

Cracking Stored Hashes:

If you can access LDAP database files or backups, hash cracking tools like hashcat can help test password strength.

Misconfigured PAM or SSSD:

Check for misconfigurations in `/etc/pam.d/` or `/etc/sss/sss.conf` that might leak sensitive information or allow bypassing authentication.

Ethical Considerations

Always obtain proper authorization before testing.

Document findings clearly to assist in remediation.

Recommend securing LDAP with:

Strong access controls.

Encrypted communication (LDAPS or StartTLS).

Regular audits of PAM and SSSD configurations.

Use of MFA (Multi-Factor Authentication).

DarkRoot - December 13, 2024, 5:27 am

cool, thanks for the info.