Hoe wordt gebruik gemaakt van LDAP Accept Query om de ontvangers van inkomende berichten te valideren met behulp van Microsoft Active Directory (LDAP)?

Inhoud

Vraag:

Hoe wordt gebruik gemaakt van LDAP Accept Query om de ontvangers van inkomende berichten te valideren met behulp van Microsoft Active Directory (LDAP)?

Opmerking: Het volgende voorbeeld wordt geïntegreerd met een standaard Microsoft Active Directory-implementatie, hoewel de principes kunnen worden toegepast op vele typen Ldap-implementaties.

U maakt eerst een LDAP server entry, waarna u uw directory server moet specificeren, evenals de query die de E-mail security applicatie zal uitvoeren. De query wordt dan ingeschakeld of toegepast op uw inkomende (openbare) luisteraar. Deze LBP server instellingen kunnen worden gedeeld door verschillende luisteraars en andere delen van de configuratie zoals toegang tot quarantaine voor eindgebruikers.

Om de configuratie van de LDAP-vragen op uw IronPort-apparaat te vergemakkelijken, raden we u aan een browser te gebruiken, waarmee u uw schema en alle eigenschappen waarop u een vraag kunt stellen, kunt bekijken.

U kunt voor Microsoft Windows het volgende gebruiken:

Voor Linux of UNIX kunt u de `ldapsearch` uit.

Eerst moet je de LDAP server definiëren om een vraag te stellen. In dit voorbeeld wordt de bijnaam "PublicLDAP" gegeven voor de server *myldapserver.voorbeelds.com* LDAP. De vragen worden gericht aan TCP poort 389 (het standaard).

OPMERKING: Als uw Active Directory-implementatie subdomeinen bevat, kunt u geen vragen stellen voor gebruikers in een subdomein met behulp van de base DN van het root-domein. Wanneer u Active Directory gebruikt, kunt u LDAP echter ook vragen tegen de Global Catalog

(GC) Server op TCP poort 3268. De GC bevat partiële informatie voor *all* objecten in het Active Directory-bos en geeft verwijzingen naar het subdomein in kwestie wanneer verdere informatie vereist is. Als u gebruikers in uw subdomeinen niet kunt "vinden", laat de basis DN bij de wortel achter en stel de IronPort in om de GC poort te gebruiken.

GUI:

1. Maak een nieuw LBP-serverprofiel met waarden die eerder vanaf uw directory server (Systeembeheer > LDAP) zijn geplaatst. Bijvoorbeeld: Naam van serverprofiel: *PublicLDAP*Host Name: *myldapserver.example.com*Verificatiemethode: *Wachtwoord gebruiken:* *Ingeschakeld*Gebruikersnaam:*cn=ESA,cn=Gebruikers,dc=voorbeeld,dc=com*Wachtwoord: *wachtwoord*Type server: *Actieve map*Port: 3268BaseDN:*dc=voorbeeld, dc=com*Gebruik de knop "Test Server(s)" om de instellingen te controleren voordat u doorgaat. Een succesvolle uitvoer moet er zo uitzien:

```
Connecting to myldapserver.example.com at port 3268
Bound successfullywithDNCN=ESA,CN=Users,DC=example,DC=com
Result: succeeded
```

2. Gebruik hetzelfde scherm om de LDAP Accessoire query te definiëren. In het volgende voorbeeld wordt het adres van de ontvanger gecontroleerd aan de hand van de meest voorkomende eigenschappen, hetzij "post", hetzij "proxyAdressaten":Name: *PublicLDAP.accepteren*QueryString: *(|(mail= {a}) (proxyAdressen=smtp: {a})*U kunt de knop "Test Query" gebruiken om de zoekresultaten voor een geldige account te controleren. Succesvolle resultaten bij het zoeken naar het adres van de servicerekening "esa.admin@example.com" moeten er zo uitzien:

```
Query results for host:myldapserver.example.com
Query (mail=esa.admin@example.com) >to server PublicLDAP (myldapserver.example.com:3268)
Query (mail=esa.admin@example.com) lookup success, (myldapserver.example.com:3268) returned
1 results
Success: Action: Pass
```

3. Pas deze nieuwe Accepteer query toe op de inkomende Luisteraar (Netwerk > Luisteraars). Uitbreidt de opties LDAP Series > Aanvaarden en kies uw query PublicLDAP.Accepteren.

4. Ten slotte, verbind de veranderingen aan om deze instellingen mogelijk te maken.

CLI:

1. **Eerst gebruikt u de opdracht *ldapfig* om een LDAP-server te definiëren zodat het apparaat zich kan binden aan, en vragen voor de acceptatie van de ontvanger (ldapAcceptie-subopdracht), routing (vertraagde subopdracht) en masquerading (maskerade-subopdracht) worden ingesteld.**

```
mail3.example.com> ldapconfig
```

```
No LDAP server configurations.
Choose the operation you want to perform:
- NEW - Create a new server configuration.
[]> new
Please create a name for this server configuration (Ex: "PublicLDAP"):
[]> PublicLDAP
Please enter the hostname:
[]> myldapserver.example.com
Use SSL to connect to the LDAP server? [N]> n
Please enter the port number:
[389]> 389
Please enter the base:
[dc=example,dc= com]>dc=example,dc=com
Select the authentication method to use for this server configuration:
1. Anonymous
2. Password based
[1]> 2
Please enter the bind username:
[cn=Anonymous]>cn=ESA,cn=Users,dc=example,dc=com
Please enter the bind password:
[]> password
Name: PublicLDAP
Hostname: myldapserver.example.com Port 389
Authentication Type: password
Base:dc=example,dc=com
```

2. Ten tweede, moet u de vraag definiëren om tegen de LDAP server uit te voeren die u net hebt ingesteld.

```
Choose the operation you want to perform:
- SERVER - Change the server for the query.
- LDAPACCEPT - Configure whether a recipient address should be accepted or bounced/dropped.
- LDAPROUTING - Configure message routing. - MASQUERADE - Configure domain masquerading.
- LDAPGROUP - Configure whether a sender or recipient is in a specified group.
- SMTPAUTH - Configure SMTP authentication.
[]> ldapaccept
Please create a name for this query:
[PublicLDAP.ldapaccept]> PublicLDAP.ldapaccept
Enter the LDAP query string:
[(mailLocalAddress= {a})]>(|(mail={a})(proxyAddresses=smtp:{a}))
Please enter the cache TTL in seconds:
[900]>
Please enter the maximum number of cache entries to retain:
[10000]>
Do you want to test this query? [Y]> n
Name: PublicLDAP
Hostname: myldapserver.example.com Port 389
Authentication Type: password
Base:dc=example,dc=com
LDAPACCEPT: PublicLDAP.ldapaccept
```

3. Zodra u de LDAP query hebt ingesteld, moet u het LDAPaccepteren beleid toepassen op uw inkomende Luistener.

```
example.com> listenerconfig
Currently configured listeners:
1. Inboundmail (on PublicNet, 192.168.2.1) SMTP TCP Port 25 Public
2. Outboundmail (on PrivateNet, 192.168.1.1) SMTP TCP Port 25 Private
Choose the operation you want to perform:
- NEW - Create a new listener.
- EDIT - Modify a listener.
- DELETE - Remove a listener.
- SETUP - Change global settings.
[]> edit
Enter the name or number of the listener you wish to edit.
[]> 1
```

```
Name: InboundMail
Type: Public
Interface: PublicNet (192.168.2.1/24) TCP Port 25
Protocol: SMTP
Default Domain:
Max Concurrency: 1000 (TCP Queue: 50)
Domain Map: Disabled
TLS: No
SMTP Authentication: Disabled
Bounce Profile: Default
Use SenderBase For Reputation Filters and IP Profiling: Yes
Footer: None
LDAP: Off
Choose the operation you want to perform:
- NAME - Change the name of the listener.
- INTERFACE - Change the interface.
- LIMITS - Change the injection limits.
- SETUP - Configure general options.
- HOSTACCESS - Modify the Host Access Table.
- RCPTACCESS >- Modify the Recipient Access Table.
- BOUNCECONFIG - Choose the bounce profile to use for messages injected on this listener.
- MASQUERADE - Configure the Domain Masquerading Table.
- DOMAINMAP - Configure domain mappings.
- LDAPACCEPT - Configure an LDAP query to determine whether a recipient address should be
accepted or bounced/dropped.
- LDAPROUTING - Configure an LDAP query to reroute messages.
[]> ldapaccept Available Recipient Acceptance Queries
1. None
2. PublicLDAP.ldapaccept
[1]> 2
Should the recipient acceptance query drop recipients or bounce them?
NOTE: Directory Harvest Attack Prevention may cause recipients to be
dropped regardless of this setting.
1. bounce
2. drop
[2]> 2
Name: InboundMail
Type: Public
Interface: PublicNet (192.168.2.1/24) TCP Port 25
Protocol: SMTP
Default Domain:
Max Concurrency: 1000 (TCP Queue: 50)
Domain Map: Disabled
TLS: No
SMTP Authentication: Disabled
Bounce Profile: Default
Use SenderBase For Reputation Filters and IP Profiling: Yes
Footer: None
LDAP: ldapaccept (PublicLDAP.ldapaccept)
```

4. Om de veranderingen te activeren die aan de luisteraar worden aangebracht, verbind uw veranderingen.