# 6.2.2 Enumeration Countermeasure Facts

We have seen the extent of the information that can be gathered through enumeration. Now, let’s examine a few countermeasures.

This lesson covers the following topics:

- SNMP countermeasures
- DNS countermeasures
- SMTP countermeasures
- LDAP countermeasures

## SNMP Countermeasures

There are several countermeasures for attacks on Simple Network Management Protocol (SNMP) processes:

| Method | Description |
|---|---|
| Monitor SNMP ports | Block or monitor activity on ports 161 and 162 and any other ports that you have configured for SNMP traffic. |
| Remove SNMP agent | Remove the SNMP agent or turn off the SNMP service completely. |
| Update SNMP | Verify that you are running the most recent version of SNMP at all times. |
| Change default passwords | Change default passwords on all devices and services. |
| Run SNScan | Use SNScan, a utility that detects network SNMP devices that are vulnerable to attack. |

## DNS Countermeasures

Use the following countermeasures to mitigate attacks that target your Domain Name System (DNS) vulnerabilities:

| Method | Description |
|---|---|
| DNS zone restriction | DNS zone restriction ensures that a server provides copies of zone files to only specific servers. |
| Digital signatures | Modern systems include digital signatures that help with DNS zone restriction. |
| Split DNS | Splitting the DNS into internal and external groups provides an added layer of security. |

## SMTP Countermeasures

The most basic way to counteract Simple Mail Transfer Protocol (SMTP) exploitation is to simply ignore messages to unknown recipients instead of sending back error messages. Additionally, you’ll want to configure your server to block open SMTP relaying.

## LDAP Countermeasures

Hardening against Lightweight Directory Access Protocol (LDAP) enumeration can be tricky. Although blocking LDAP port 389 is an option, you can’t always block ports, or you’ll risk impacting your network. Blocking LDAP ports could prevent your clients from querying necessary services. The best way to secure LDAP is to review and implement the security settings and services available with your server software.