4.2.7 Reconnaissance Countermeasure Facts

This lesson covers the following topics:

- Information sharing policies
- DNS countermeasures

Information Sharing Policies

Policy	Description
Internet	Review company websites to see what type of information is being shared about sensitive information. Opt out of archiving sites.
Company social media	Provide guidelines regarding the types of posts that are made to the company's social media site.
Employee social media	Implement policies that restrict the sharing of sensitive company information on an employee's personal social media page. This could include product information, customer or vendor information, employee information, or even pictures of the organization.
Printed materials	Limit the sharing of critical information in press releases, annual reports, product catalogs, or marketing materials.

DNS Countermeasures

DNS is one of the most popular internet services targeted during the reconnaissance phase. It goes without saying that we should harden our servers. Failure to do so could result in far bigger problems than just providing too much information to the outside world.

Even the strongest security features are only as good as their implementation, so you'll want to be sure to learn as much as you can about your web server software and verify that you're optimizing your resources to their full potential. After you've set everything up, your work is far from over. Hackers are always working to find new ways to access your system, and you'll want to work just as hard to keep your DNS servers up to date. This means installing patches against known vulnerabilities, cleaning up out-of-date zones, files, users, and groups, and, of course, running your own vulnerability tests.

You may also want to consider a split DNS. With the increase in the number of remote access and cloud-based applications, this solution is becoming more common. Using this method, clients accessing the DNS server from the internet receive public IP addresses, and clients inside the company's network receive internal IP addresses. Clients with the internal IP addresses can be granted access to more secure content than the clients with the external IP addresses.