4.1.2 Reconnaissance Process Facts

Reconnaissance is a systematic attempt to locate, gather, identify, and record information about a target.

This lesson covers the following topics:

- Information types
- Information gathering techniques
- Permission and documentation

Information Types

During the reconnaissance phase, you gather information about a company. In addition to technical information, you'll want to gather details about employees, vendors, business processes, and physical security.

Information	Description
Employees	Contact names, phone numbers, email addresses, fax numbers, addresses for any individuals associated with the target company
Physical security	Geographical information, entry control systems, employee routines, and vendor traffic
Vendors	Names, contact information, and account numbers
Operations	Intellectual property, critical business functions, and management hierarchy
Information systems	Operating systems, applications, security policies, and network mapping

Information Gathering Techniques

During the reconnaissance phase, you gather information by reading a company's website, getting to know their employees, or dumpster diving.

Method	Description
Websites	You can research company websites, social media, discussion groups, financial reports, and news articles. If you follow the breadcrumbs, you can find some pretty interesting things about an organization online.
Social engineering	Social engineering is an attempt to get to know the employees or the vendors of the company. After-work social gatherings can provide important tidbits of information about an employee and about a company, especially its weaknesses.
Dumpster diving	Despite our highly technical society, dumpster diving is still an option to consider. Let's be honest; it's not the most glamorous method. But, in some instances, it may be very effective for finding employee names, account numbers, client names, and vendor information.
Social networking	After you've located employee names, you can extend your search to LinkedIn, Facebook, Instagram, Twitter or People Search to learn even more information about a company, a vendor, or an employee.

Permission and Documentation

The difference between an ethical hacker and a criminal hacker is that the ethical hacker always obtains permission. Before beginning work of any kind, an ethical hacker needs to obtain written documentation granting permission from the customer. They should verify that the agreement specifies the scope of the assessment and any guidelines or limitations that may be in place.

As with any technical project, you will need to thoroughly document your findings. Recording information while it's fresh in your mind reduces the potential for errors or missing details.