2.3.3 Target Selection Facts

Before beginning a penetration test, there are a lot of details that must be worked out. These details include the type of test being performed and any test limitations. After the initial plans and details for a penetration test have been put together, there are some additional details that should be considered. These include performing a risk assessment, determining tolerance, scheduling the test, and identifying security exceptions that may be applied to the penetration tester.

This lesson covers the following topics:

- Penetration test planning
- Security exceptions
- Risk assessment
- Determine tolerance
- Scope creep

Penetration Test Planning

Detail	Description
How	One of the first items to consider is the type of test to be performed, internal or external. An internal test focuses on systems that reside behind the firewall. This would probably be a white box test. An external test focuses on systems that exist outside the firewall, such as a web server. This would, more than likely, be a black box test.
Who	Determine if the penetration tester is allowed to use social engineering attacks that target users. It's common knowledge that users are generally the weakest link in any security system. Often, a penetration test can target users to gain access. You should also pre-determine who will know when the test is taking place.
What	The organization and the penetration tester need to agree on which systems will be targeted. The penetration tester needs to know exactly which systems are being tested, and as they cannot target any area that isn't specified by documentation. For example, the organization may have a website they do not want targeted or tested. Some other systems that need to looked at include wireless networks and applications.
When	Scheduling the test is very important. Should the test be run during business hours? If so, this may result in an interruption of normal business procedures. Running the tests when the business is closed (during weekends, holidays, or after-hours) may be better, but might limit the test.
Where	Finally, will the test be run on site, or remotely? An on-site test allows better testing results, but may be more expensive than a remote test.

Security Exceptions

A security exception is any deviation from standard operating security protocols. The type of test (white box, black box, grey box) will determine what, if any, security exceptions the penetration test will be given.

Risk Assessment

The purpose of a risk assessment is to identify areas of vulnerability within the organization’s network. The risk assessment should look at all areas, including high value data, network systems, web applications, online information, and physical security (operating systems and web servers). Often, the penetration test is performed as part of a risk assessment.

Once vulnerabilities have been determined, the organization needs to rank them and figure out how to handle each risk. There are four common methods for dealing with risk:

1. Avoidance: whenever you can avoid a risk, you should. This means performing only actions that are needed, such as collecting only relevant user data.
2. Transference: the process of moving the risk to another entity, such as a third party.
3. Mitigation: this technique is also known as risk reduction. When the risk cannot be avoided or transferred, steps should be taken to reduce the damage that can occur.
4. Acceptance: sometimes the cost to mitigate a risk outweighs the risk's potentially damaging effects. In such cases, the organization will simply accept the risk.

Determine Tolerance

After the risk assessment has been performed and vulnerable areas are identified, the organization needs to decide its tolerance level in performing a penetration test. There may be areas of operation that absolutely cannot be taken down or affected during the test. Areas of risk that can be tolerated need to be placed in the scope of work, and critical areas may need to be placed out of the test's scope.

Scope Creep

In project management, one of the most dangerous issues is scope creep. This is when the client begins asking for small deviations from the scope of work. This can cause the project to go off track and increase the time and resources needed to complete it. When a change to the scope of work is requested, a change order should be filled out and agreed on. Once this is done, the additional tasks can be completed.
