Penetration Tester

A Penetration Tester is an essential role in cybersecurity that searches for insecurities within an app, website, or other digital areas of a company. They do this by finding insecurities in the company, exploiting them, and documenting the findings in a report for the company. They use creative ways to find issues within the digital space, and work from the outside in.

The 5 main duties of the job are as follows:

1. Communicate with the client and your team to collaborate on projects. You are often working in large teams and need to communicate everything you do.
2. Use reconnaissance by investigating subdomains, servers, and IP's to find entries into a company's system. By doing so you are making a layout of the target and possible weak points.
3. Know how to use scanning software and other digital cybersecurity products. Pentesting requires a variety of software and digital products as a toolbox for the tester.
4. Exploit the company's weaknesses and get into their system without compromising the information. This is the part you document for the client and give advice for the next steps.
5. Properly document the findings and give advice for the company's next steps. You need to be specific and brief in your documentation because many of your clients don't have technical expertise.

The required skills for this job are as follows:

1. Soft skills in communication and collaboration. This includes time management, presentation skills, and documentation skills.
2. Proficiency in coding languages like Python, Javascript, SQL, and Powershell. Additionally, you will need to be able to learn new libraries for these languages and constantly update your skillset.

3. Ability to use software such as Nmap, Burp Suite, and Linux. This software is crucial for pentesting and varies based on what you are testing.
4. Extensive knowledge on OS systems, Networks, and the Cloud. This is the most important part of being a pentester as you need to know your way around the digital space.
5. Problem solving abilities and being able to think outside the box. This is needed because you have to think like a hacker to properly pentest the client.

Some common deliverables for this job are as follows:

1. The largest and most important deliverable for a pentester is the penetration test report. It is the main document that is given to the client when the test is done; explaining the exploits found, the impact it has, and next steps to fix it.
2. Another important deliverable is the client debrief. The debrief is a meeting or email conversation with the client to explain to them what testing you are going to do and answer any of their questions.
3. A technical output/ testing log is similar to a pentest report, but has more technical info instead of easy to read reports. It often has screenshots of software outputs, commands used, and network captures.
4. During pentesting, you often work with a team and need to communicate your actions/discoveries. This team briefing can be daily, weekly, or as needed.
5. Another table that is less used is a risk summary table. A risk summary table is a visual overview of the vulnerabilities and the risk they pose to the client. These are important because it gives the client a better idea of the severity for each vulnerability.

Some common work environments or company types a pentester works in is as follows:

1. A common work environment for a pentester is a consulting firm. A consulting firm hires pentesters and finds clients for them. This style has the most consistent work and is a fast paced environment. The downsides would be the lack of flexibility within the work schedule.

2. An in-house red team is a team of pentesters that are hired by the company and work internally. This is usually reserved for large companies with the need and budget for an in-house team. This style has substantial pay and more control over the projects, though it is difficult to find openings.
3. A bug bounty hunter is a freelance pentester that uses sites like HackerOne to find companies that will pay you to find vulnerabilities. This line of work has infinite flexibility though usually doesn't pay as well as firms or in-house teams.

Some common work rigors and growth styles are as follows:

1. For a consulting firm there is an intermediate amount of growth with lots of exposure into the industry. For the entry level positions you will be able to get experience and move firms if needed. For intermediate positions you can manage teams at the firm and spend more time talking to clients. For advanced positions there are a couple of options, though often they start their own firm and find clients for their team.
2. For an in house team there are many places to grow throughout the company and even move laterally. For entry level positions, you'll find yourself completing tasks assigned by your manager,and attending meetings. For intermediate positions you may become a project manager or specialist. For advanced level positions, you will be moving up the corporate ladder and may even move away from cybersecurity.
3. For a bug bounty hunter there is not a lot of professional area for growth as most of the work is self directed. An entry level hunter can find smaller bugs and may not make a substantial income. For intermediate, you may find larger bugs and start making a living from finding the bounties. For advanced, you will most likely find the largest bounties and may start blogging, attending events, and start building a name for yourself professionally.