Hack the Cybersecurity Interview

A complete interview preparation guide for jumpstarting your cybersecurity career

Ken Underhill | Christophe Foulon | Tia Hopkins

Foreword by Mari Galloway, CEO, Founding Board Member of Women's Society of Cyberjutsu

Hack the Cybersecurity Interview

A complete interview preparation guide for jumpstarting your cybersecurity career

Ken Underhill

Christophe Foulon

Tia Hopkins

Packt

BIRMINGHAM—MUMBAI

Hack the Cybersecurity Interview

Every effort has been made in the preparation of this book to ensure the accuracy of the information presented. However, the information contained in this book is sold without warranty, either express or implied. Neither the authors, nor Packt Publishing or its dealers and distributors, will be held liable for any damages caused or alleged to have been caused directly or indirectly by this book.

Packt Publishing has endeavored to provide trademark information about all of the companies and products mentioned in this book by the appropriate use of capitals. However, Packt Publishing cannot guarantee the accuracy of this information.

Group Product Manager: Vijin Boricha

Publishing Product Manager: Mohd Riyan Khan

Senior Editor: Athikho Sapuni Rishana

Content Development Editor: Sayali Pingale

Technical Editor: Arjun Varma

Copy Editor: Safis Editing

Associate Project Manager: Neil Dmello

Proofreader: Safis Editing

Indexer: Subalakshmi Govindhan

Production Designer: Alishon Mendonca

Marketing Coordinator: Sourodeep Sinha

Senior Marketing Coordinator: Hemangi Lotlikar

First published: July 2022

Production reference: 1010722

Published by Packt Publishing Ltd.

Livery Place

35 Livery Street

Birmingham

B3 2PB, UK.

978-1-80181-663-2

`www.packt.com`

Contributors

About the authors

Ken Underhill is the executive producer and host of the syndicated Cyber Life® television show, which reaches millions of viewers each month around the world on the Binge Networks app, Amazon, Roku, and over 100 other streaming television channels. He has won multiple industry awards for his work to improve diversity in the industry and is an advocate for women's rights. Ken educates around 2.6 million people each year through his online cybersecurity courses, is an executive and business owner, and sits on the advisory board of **Breaking Barriers Women in Cybersecurity** (**BBWIC**) and the Whole Cyber Human Initiative, along with sitting on the board for a number of cybersecurity start-up companies.

I would like to thank my co-authors, Chris and Tia, for agreeing to do this book and sharing their wisdom with the world. I would also like to thank Mari Galloway for agreeing to join us on this book journey. Thanks to our technical editors for surfacing new perspectives as we wrote this book.

Christophe Foulon, senior manager and cybersecurity consultant at F10 FinTech, brings over 15 years of experience as a vCISO, information security manager, adjunct professor, author, and cybersecurity strategist with a passion for customer service, process improvement, and information security. He also has spent more than 10 years leading, coaching, and mentoring people. As a security practitioner, Christophe is focused on helping businesses tackle their cybersecurity risks while minimizing friction, resulting in increased resiliency, and aiding to secure people and processes with a solid understanding of the technology involved. He also hosts the Breaking into Cybersecurity podcast and co-authored *Develop Your Cybersecurity Career Path*.

I would like to acknowledge the staff, editors, and co-authors who have guided me through the process of writing this book. I would also like to thank the readers of these books who support authors like us and then give back by helping those who follow behind them by recommending resources and sharing experiences to keep this cycle going.

Tia Hopkins is the field CTO and chief cyber risk strategist at eSentire. She is also an adjunct professor of cybersecurity at Yeshiva University, a football coach, and is pursuing an executive MBA and Ph.D. in cybersecurity.

Tia was recognized by SC Media as an outstanding educator in 2019, as well as one of the Top 25 Women Leaders in Cybersecurity and Top 100 Women in Cybersecurity, both in 2020. In 2021, Tia was recognized as a Top Influencer in the Security Executives category by IFSEC Global. She also contributed a chapter to the book *The Rise of Cyber Women: Volume 2*.

Tia is the founder of Empow(H)er Cybersecurity, a non-profit organization aimed at inspiring and empowering women of color to pursue cybersecurity careers.

I would like to thank Ken for inviting me to join him and Chris on this amazing journey. I would also like to thank all of our supporters for believing in the value of this book, and I look forward to your feedback on how it helped you in your cybersecurity career journey. Don't forget to pay it forward!

About the reviewers

Linda W. Bell, CISSP, CDPSE, is a security architect and compliance lead for IBM Security Verify, with over 15 years of experience in risk management and accounting. After serving as a cybersecurity engineer in the Global CISO organization, she transitioned to resiliency advisor in the IBM Security BISO. There, she provided expertise in business continuity program management and incident response. Linda is a sought-after speaker on security topics and has been interviewed by several publications and organizations. Outside of work, Linda mentors underrepresented groups to help them attain certifications or training for STEM-based careers. She holds a Bachelor of Science degree in information technology from the University of South Florida.

I'd like to thank my family for supporting me over my career. Technology requires lifelong learning to stay current and I appreciate their patience when I am studying over weekends or for certifications. Also, a big thanks to all the women who sent the elevator back down and opened doors for me to be able to tell my STEMstory.

Louis Anthony Maldonado Jr has worked in various areas of cybersecurity. As a lead analyst for critical infrastructure at Duke-Energy, Louis has stood up and matured command centers, directed EDR assessments overseas, and trained global security operations centers on monitoring and response. He was a consultant at multiple international agencies representing SOAR integrations and automation for various clients. Currently at Pacific Gas and Electric across the United States and back in critical infrastructure, Louis is maturing his department's cybersecurity posture. Louis is a leader among his peers and has a strong presence in the industry.

I'd like to thank my mother, Patricia, who never gave up on me and continued to push me to pursue my passion. Thanks to my two boys, Louis and James, as they unknowingly fueled my career and growth. Thanks to the authors of this book, allowing others to obtain this knowledge and grow their careers. Thanks to my colleague George from Blak Cyber, who referred me to Packt, and my contacts at Packt who kept me focused. Cheers!

3
Penetration Tester

In this chapter, you will learn what a **penetration tester** (**pentester**) is and the average salary range for this career in the **United States** (**US**). You will also learn about career progression options and learn common interview questions for the role.

The following topics will be covered in this chapter:

- What is a pentester?
- How much can you make in this role?
- Which other roles can you do?
- Common interview questions for a pentester career

What is a pentester?

Penetration testing (**pentesting**) or ethical hacking is where you assess the security of networks, websites, endpoints, mobile devices, wireless devices, **operational technology/industrial control system** (**OT/ICS**) infrastructure, and the security of physical facilities. This assessment might include performing vulnerability scanning and analysis, reviewing source code, performing **open source intelligence** (**OSINT**), gaining access to a target by exploiting vulnerabilities, escalating privileges, maintaining persistence, and more.

A key thing here is that you have permission as a pentester to attack the target as defined in the **statement of work** (**SOW**) of the **penetration test** (**pentest**). If you don't have permission, then it's illegal. Before starting action on any pentest, you need to review the **rules of engagement** (**ROEs**) and determine the scope of the pentest and verify that the client owns everything listed. I've reviewed SOWs before where the client mistyped an **Internet Protocol** (**IP**) address and we could have been in legal trouble for performing the pentest if we had not corrected the documentation. The right documentation is like a get-out-of-jail-free card during a pentest.

A goal of pentests is to simulate which vulnerabilities are exploitable by an adversary, and this is where vulnerability assessments and pentests differ. A vulnerability assessment just identifies that there might be something an adversary can exploit, and a pentest shows that it can be exploited and provides ways to mitigate the impact.

A good way to think of the difference between vulnerability assessments and pentesting is a car. Your mechanic runs a diagnostic scan (vulnerability assessment) on your car and identifies some error codes that tell the mechanic five problems that might be the cause. The mechanic then tinkers under the hood and manually assesses those potential problems (pentest), and ultimately determines the root cause. For example, you turn on the ignition on your car, but it just will not catch and actually start the car. This could be caused by the battery, ignition switch, spark plugs, or other parts. Your mechanic runs a diagnostic scan that will indicate all of these as potential issues and then checks each one to identify what the real problems are and provides recommendations to fix them (pentest).

There are many different areas of pentesting that you can specialize in, including applications (web apps, cloud, thick clients, mobile apps, and so on), infrastructure/networking, ICS, physical, red team, hardware, **Internet of Things** (**IoT**), and social engineering. Many pentesters specialize in one or two of these areas and then also have knowledge and skills in other areas. No one is an expert in every area of pentesting, contrary to what you might see in the movies. Speaking of movies, real pentesting has nothing to do with wearing a hoodie in your mom's basement as binary code scrolls across the computer screen. Real-life pentesting takes careful planning and doesn't always involve you being an expert in computer programming, but it can be challenging and rewarding.

So, what skills do you need to be a pentester? For soft skills, passion and the ability to communicate the results of your pentest to stakeholders are critical. For technical skills, you need to have a solid foundation in operating systems, networking, and security.

The good news is that, as with most cybersecurity careers, you don't need a college degree or certifications to become a pentester.

If you are looking to gain hands-on experience with home labs, you can download VirtualBox (`https://www.virtualbox.org/`) or VMware Workstation (`https://www.vmware.com/products/workstation-player/workstation-player-evaluation.html`) for free and install Kali Linux (`https://www.kali.org/`) and Metasploitable (`https://sourceforge.net/projects/metasploitable/`) to practice. You can also find free Microsoft Windows (`https://www.microsoft.com/en-us/evalcenter/`) **International Organization for Standardization** (**ISO**) images here to build Windows **virtual machines** (**VMs**).

Heath Adams who is a professional pentester also has free ethical hacking video training on YouTube. PortSwigger (`https://portswigger.net/web-security`) also has some free training for web application pentesting. If you just do a quick search online for *ethical hacking training* or *penetration testing training*, you should find hundreds of free and low-cost resources to help build your skills.

How much can you make in this role?

The salary range for a pentester in the US depends on a number of factors, such as your location, the size of the company you work for, certifications you hold, college degrees, and your skills. I've seen salaries as low as $76,000 and as high as $270,000+ for specialized public sector work. For a junior-level pentester, you can usually expect between $70,000 and $100,000, depending on the factors I mentioned before. I do want to mention that there are far more jobs available on the defensive side of the house versus the offensive.

Which other roles can you do?

A career as a pentester means you have mastered certain technical and soft skills, so it can help prepare you for any new roles in the industry. I've typically seen pentesters move into other types of pentesting (that is, application instead of infrastructure) or move into leadership roles in the C-suite.

Common interview questions for a pentester career

The questions that follow are primarily knowledge-based questions. During a junior pentester interview, you will likely experience many knowledge-based questions, with some hands-on testing assessments possible. For senior and principal pentester job interviews, you often receive a hands-on test of your pentesting skills after the initial phone screen from the recruiter or **human resources** (**HR**). You're likely to encounter questions similar to these:

- **Where do you go to research the latest vulnerabilities, and why?**

  Your answer could include following specific security researchers on Twitter, following blogs such as Krebs and Threatpost, podcasts you listen to, and more. There isn't usually a wrong answer here, but the interviewer does want to see how you stay current on recent vulnerabilities and the latest cybersecurity news.

- **Do you have a favorite hacker in history, and why are they your favorite?**

  This question is asked to see how passionate you are about the history of hacking. This is another question with no wrong answer, and you might not have a favorite, which is OK. An example of a famous hacker in history is Kevin Mitnick.

- **What are some areas you are planning to improve in?**

  This question is being asked to see whether you are a continuous learner and to see how you identify areas of self-improvement. Even as a junior pentester, you should expect to be learning something new continuously, and you need to be able to assess your skill set and know the areas you need to improve in. For example, I'm good at social engineering but not so good at programming. As a pentester, I focused less practice on social engineering since that came naturally and focused instead on becoming better at coding so that I could write my own tools.

- **I need you to perform an internal pentest and I have an ROE document in place. What do you do next?**

  The interviewer is identifying your methodology for approaching a pentest with this question. If you're interviewing for your first pentesting job, you always want to make sure you review and verify the ROE (scoping) document to know what is off limits and what you can attack. Clients sometimes list wrong IP addresses, so you also need to verify that anything listed as available to attack is actually owned by the client. Otherwise, you can get yourself into legal trouble.

- **What are the types of cross-site scripting (XSS), and which is the most dangerous?**

  There are three types of XSS, which are reflected, stored, and **Document Object Model** (**DOM**)-based. The specific danger of each depends on the situation. Stored XSS is typically more dangerous because it is stored on the server side and the payload only has to be stored once to continue infecting anyone connecting to the server.

- **Can you explain XSS as though you were talking to a 10-year-old kid?**

  This question is designed to see whether you can break down complex cybersecurity topics for stakeholders. Here in the US, statistics vary, but most people understand it at an 8th-grade level or below, which means you have to communicate information to stakeholders as though they are 10-year-old kids in many situations. I would explain this one with something like this statement:

  With XSS, you can log in to anyone's account with a username and password. This is important to fix because an attacker can use attacks such as XSS to perform illegal transactions, which can lead to the company losing money.

  When you're presenting to corporate stakeholders, you can also mention how XSS can lead to cookie stealing and be used to perform privilege escalation and in phishing attacks.

- **How can you perform XSS if <script> or alert tags are blocked?**

  If `<script>` tags are blocked, you could use things such as image payloads or video payloads. Instead of using `alert` tags, you could use tags such as `prompt` and `confirm`.

- **What are some ways to mitigate XSS attacks?**

  You can use encoding, validate user input properly, sanitize output, and use **web application firewalls** (**WAFs**).

- **What was the last script that you wrote, and what was its purpose?**

  I want to stress here that as a junior pentester, you don't have to have coding skills, but if you want to be successful in the long term, it's important for you to learn at least one language so that you can write new tools on the fly during an engagement. This question is used to assess your scripting skills, and you might write something simple such as a keylogger that you can show off during the interview.

- **What are some types of threat actors?**

  This question is usually looking for your broader knowledge of threat actors, so mentioning nation-state groups, state-sponsored groups, hacktivists, organized criminal gangs, script kiddies, and insider threats is good for this question. It's also a good idea to stay current on cybersecurity breaches and the threat actors behind them, or at least know a few of the well-known threat actor groups (that is, *APT29*) from searching a website such as the *MITRE* **Adversarial Tactics, Techniques, and Common Knowledge** (**ATT&CK**) website.

- **How do you scope out a pentesting engagement?**

  The first step is typically determining why the company wants a pentest. Are they just doing the engagement to fulfill some type of legal or compliance requirement? Does the organization have an initiative to improve overall organizational security? Knowing why they want the pentest helps you understand how much buy-in you will have from their team.

- **What are some ways you can gather information on a target during a pentest?**

  Some of the common ways to get information on a target include more passive activities, such as OSINT, and more active techniques, such as running a **Network Mapper** (**Nmap**) scan. Your specific actions will depend on the scope of the pentest. If you get this question in an interview, I would suggest asking a question back to the interviewer about the scope of the pentest because that will help guide your answer to this question.

- **What is social engineering?**

  Social engineering is basically the use of human psychology to influence someone else's behavior.

  Components of a successful social engineering attack include an evaluation of the target and their weaknesses, the ability to perform pretexting, the ability to exploit human psychology for the attacker's benefit, the ability to build a perceived relationship with the target, and the ability to get the target to take some sort of desired action.

Here's a simple example of social engineering. You and I are at a coffee shop, and I convince you to buy me a cup of coffee. Perhaps I mention I left my wallet at home because I'm stressed out that my kid is in hospital, and you feel sorry for me and buy the cup of coffee because you have little kids of your own. In this example, I'm just getting a cup of coffee, but what if I sent you an email with a malicious GoFundMe link embedded with a keylogger and used the same story about my kid in the hospital? You might click the link to donate, be redirected to the real GoFundMe page, and make a donation to help. Meanwhile, I've dropped malware on your system and now track every keystroke you make as you log in to your bank account to see whether the GoFundMe donation has registered on your account balance.

One thing to keep in mind is that during an interview, you might be asked to conduct a social engineering attack and then continue your (simulated) attack through the organization after gaining initial entry. The next steps after entry can include things such as enumerating user accounts on the system to identify administrator accounts, privilege escalation, network enumeration, deploying ransomware, and enumerating Active Directory with a tool such as BloodHound (`https://github.com/BloodHoundAD/BloodHound`).

- **What are some ways to perform physical pentesting?**

Before answering this question, it's usually best to start with a short overview of what could happen if physical security were breached. If you breach the physical security of a target, you could steal devices, documents, and data, take photographs or videos of restricted areas or proprietary systems and additional security defenses being used to protect them, and then plant things such as keyloggers (via a **Universal Serial Bus** (**USB**) drop attack) and set up rogue devices on the target's network.

Common physical security controls that are put in place to stop attackers include door locks (physical/electronic), surveillance cameras and security alarms, security guards, perimeter walls and gates, security lights, motion sensors, and mantraps.

Physical pentesting can include dumpster diving, lock picking, cloning badges, bypassing motion detectors, jumping fences or walls, bypassing or interrupting the feeds of surveillance, cameras, and **radio-frequency identification** (**RFID**) replay attacks.

- **What are the types of social engineering?**

  There are several types of social engineering attacks, including the following:

  - **Phishing attacks** are typically done via email whereby the attacker is looking to obtain sensitive information or get the recipient to perform a specific action (such as transfer money to a bank account controlled by the attacker). There are several forms of phishing attacks, such as these:

    - **Phishing emails** are the most common form of phishing attacks, and you will typically see them done against a broad range of targets—in the case of spam—or more narrowly focused—in the case of **business email compromise** (**BEC**) attacks. BEC attacks usually involve spear-phishing and whaling. Phishing attacks are the most common entry point of attacks, including ransomware attacks.

    - **Spear-phishing attacks** are targeted phishing attacks against a specific person or group. The attacker would need to gain information about the target and craft a message, across any medium, that would entice the victim to take some sort of action. An example would be the attacker knowing you love drinking coffee from Starbucks. Through social media posts, the attacker identifies two locations you typically go to and then sends you a coupon link through social media for a free cup of coffee at one of those locations. In one of my training programs, a student was able to get an instructor to click a fake link with a similar type of attack for a free donut. Fortunately for the instructor, this was done in a controlled setting and the link was not really malicious.

    - Another example of a spear-phishing attack is the threat actor noticing employees at a company order from the same restaurant at lunch each day and then compromising the restaurant's website with malware so that each employee visiting the website gets their system infected. This is known as a **watering-hole attack**.

    - **Whaling attacks** are another form of a targeted phishing attack. The main difference between whaling attacks and spear-phishing attacks is that a whaling attack focuses on a powerful or wealthy individual, such as the **chief executive officer** (**CEO**) of a major company. A whaling attack is often harder to pull off successfully, but the financial reward for the attacker could be in the millions.

- **Tailgating** is another social engineering attack where the adversary gains access to a secure area by following an authorized employee in. In this case, the employee does not know the attacker has followed them in, and this can happen if the employee opens the door wide or if it takes time for the door to close after the authorized employee. This attack is hard to pull off if there are security guards or if the authorized employee is situationally aware.
- **Piggybacking** is an attack whereby the victim is tricked into letting the attacker in. This can happen a lot at larger companies, where the attacker mentions they work in a different department and just forgot their badge at home. Forgetting a badge or other employee ID happens a lot in companies, and many employees would empathize with the attacker and let them in the door.

  I worked at a healthcare organization where every day, someone would forget their badge to scan in and wait at the door for someone else to let them in. Even back then, I implemented zero trust and would decline to let the person in, even if they worked in my department. My argument was that I didn't know whether HR had fired them last night and they were unauthorized to be in the building. Needless to say, that didn't make me popular with some coworkers, but they did understand my point of view a few months later when a man with a gun was able to gain entry into the building because someone else thought he worked there and had just forgotten his badge.

  Some other attacks you might see referenced in certification study material are hoaxes, elicitation, spam, and impersonation. In my experience, these are normally coupled with the previous ones mentioned. For example, a hoax is simply where the attacker presents a fictitious situation. An example of this is when you receive a phishing email from your *bank* stating there is an issue with your account, and you need to verify your identity by logging in to your account from a link in the email. If you click the link, you are taken to a fake login page that will capture your username and password.

- **How can a company protect against social engineering attacks?**

  Some ways to help protect against social engineering attacks are **two-factor authentication** (**2FA**), security awareness training, granular access control, logical controls (such as blocking USB ports on hosts), and proper security policies.

  When I did security awareness training for healthcare companies, I would always relate each recommendation to how it impacted the employees' day. For example, I would ask the nursing staff what would happen to their license if they shared their login credentials with me and I went in and altered 90% of their nursing notes on patients. How would they know which notes I had altered? What would local, state, and federal agencies do to them and their license? How would it impact their patients and the care that they received? When you put training into context for people, they are more likely to follow best practices.

- **What is the content of a well-written pentest report?**

  A pentest report is important and should contain the following items:

  - A cover page.
  - An executive summary should be one page or less and should highlight exciting pieces of the report's findings. Think of this part as marketing, and you need to get the stakeholder to buy what you are selling so that they finish reading the full report.
  - A summary of vulnerabilities that you found. A simple pie-chart graphic works well for this if you categorize the vulnerabilities.
  - Details of the testing team and tools that were used in the engagement.
  - A copy of the original scope of work that was signed as part of the contract. It's helpful to have this in the report as a reference for the client.
  - The main body content of the report that goes into detail in terms of your findings.

- **How can you identify whether a web application that you came across might be vulnerable to a blind Structured Query Language (SQL) injection attack?**

  You can use the `sleep` command, and if the web app sleeps for a period of time, it could indicate it is vulnerable.

- **What is a MITM attack?**

  In a **man-in-the-middle** (**MITM**) attack, the attacker acts as a relay between the client and the server. You can use things such as **HyperText Transfer Protocol (HTTP) Strict Transport Security** (**HSTS**) and digital signatures of packets to protect against MITM attacks. Some popular tools for performing MITM attacks are Wireshark, Ettercap, Nmap, Metasploit, and Netcat.

- **What is CSRF?**

  Cross-Site Request Forgery (**CSRF**) attacks take advantage of the trust relationship that is established between the user and a website. The attacker uses stored authentication in browser cookies on the user's side to authenticate to the website. An example is you have a login to a shopping website and you store the authentication in cookies in your web browser so that each time you visit the shopping website, it authenticates you and takes you into your account. An attacker could craft a **Uniform Resource Locator** (**URL**) with a parameter to increase the number of items added to your shopping cart when you are purchasing an item. You might not notice this and end up purchasing the additional items.

- **What is an open redirect attack?**

  In an open redirect attack, the parameter values of the HTTP `GET` request allow information to be entered that can redirect the user to a different website. The redirect could happen once on the loading of the website page or after the user has taken an action such as logging in to the site.

  In this example, the `RelayState` parameter is not being validated by the website, so an attacker could replace the legitimate website with their malicious one and the user would be redirected to the malicious site.

  Correct URL: `https://www.microsoft.com/login.html?RelayState=http%3A%2F%2FMicrosoftGear.com%2Fnext`

  Attacker URL: `https://www.microsoft.com/login.html?RelayState=http%3A%2F%2FBadGuyWebsite.com`

  This type of attack is commonly used in phishing emails, where the victim is redirected to a fake login page (for their bank, PayPal, and so on) after clicking a link in the email. After they enter their login credentials, the victim is then redirected to the real website and asked to enter their login credentials again.

- **Which cookie security flags exist?**

  The `HttpOnly` flag can be used to block access to the cookie from the client side, which can mitigate XSS attacks.

  The `Secure` flag forces cookies to be transported over **HTTP Secure** (**HTTPS**) instead of HTTP.

- **How do you bypass common file upload restrictions in web applications?**

  One way to bypass restrictions is using Burp Suite to intercept and alter the request parameters to bypass the restriction.

- **What is the last pentest tool that you've improved, fixed, and/or contributed to?**

  This question is targeted toward experienced pentesters, and it's designed to help the hiring manager identify how you are giving back to the community.

- **What is a Boolean blind SQL injection attack?**

  In a Boolean blind SQL injection attack, the attacker sends a SQL query to the database to identify a `true` or `false` response. If the database is vulnerable to a SQL injection attack, it will not return any information, and the attacker can then send a query with a `true` condition, such as `1=1`.

- **If you were able to successfully carry out the preceding blind SQL injection attack and gained access to the company network, where would you go from there?**

  This question is designed to test your methodology. After gaining initial access and establishing a shell, I would enumerate the **domain controllers** (**DCs**) and domain using something such as BloodHound. Next, I would dump local password hashes and do a password spray attack (using something such as Mimikatz) to gain access to a machine with a domain admin token. I would then establish a session with a DC and dump credentials to gain domain account admin access and then continue causing chaos from there. A domain admin account allows me to control virtually anything that is integrated with or controlled by Active Directory.

- **Can you identify the most common HTTP methods and how they can be used in attacks against web applications?**

  Common HTTP methods include `GET`, `POST`, `PUT`, `DELETE`, and `TRACE`. `GET` and `POST` are used in attacks by modifying the parameters. An attacker could use `PUT` to upload arbitrary files on the web server. `DELETE` could be used in a **denial-of-service** (**DoS**) attack. `TRACE` could be used to return the entire HTTP request, which would include cookies. An attacker could leverage `TRACE` to perform a **cross-site tracing** (**XST**) attack where the attacker uses XSS to retrieve `HttpOnly` cookies and authorization headers.

- **What are the differences between attacking a web application and an application programming interface (API)?**

  Web applications have traditionally been one request to one server, so you just needed to protect one application. With APIs, you have hundreds of requests to hundreds of microservices, which means you now have to protect hundreds of small applications. The main API security flaws being exploited are around authentication and authorization, and each microservice needs to verify identity and permissions before granting access. A challenge in API security is visibility into your APIs because shadow APIs might exist (those that developers have forgotten about), and if they are public-facing, they can be exploited.

- **Describe the last business logic vulnerability that you found.**

  Business logic vulnerabilities are weaknesses in the design and/or implementation of an application. An example of a business logic vulnerability is an application that cannot handle unexpected input from a user properly, such as a banking application that allowed a negative value when transferring money between accounts. An attacker might then leverage this vulnerability to remove money from the victim's account.

- **How do you measure the results of a pentest?**

  It depends on what the organization is looking to measure. Common things to track are the criticality of findings, how many issues that surfaced in the pentest actually get fixed, what types of vulnerabilities and exploits are being discovered, and which new issues have been identified since the last pentest.

- **What are the phases of pentesting?**

  This question could have different answers, depending on the hiring manager having real pentesting experience or just passing a few knowledge-based certification exams.

If you go by the **penetration testing execution standard** (**PTES**), there are seven phases of pentesting, which are *pre-engagement*, *intelligence gathering*, *threat modeling*, *vulnerability analysis*, *exploitation*, *post-exploitation*, and *reporting*.

If you take a popular knowledge-based certification exam, the phases are *reconnaissance*, *scanning and enumeration*, *gaining access*, *maintaining access*, and *covering tracks*.

- **How can you leverage threat modeling in a pentest?**

  Threat modeling helps the pentester identify critical business assets and the impact on the organization if those assets are compromised by an attacker. It also helps you identify threat actors most likely to target the organization. This helps the pentester better prioritize vulnerabilities found during the engagement.

- **Compare bug bounty programs and a pentest.**

  Bug bounty programs can typically find more vulnerabilities over time than a pentest because they involve continuous testing. You will also get a more diverse group of skill sets, and the payouts of many bug bounty programs are far less than the cost of a single pentest.

- **What is an HTTP Desync attack?**

  HTTP Desync attacks abuse the method in which a chain of HTTP servers interpret consecutive requests, especially around the boundaries of requests. As an example, an attacker could send a request with a transfer-encoding header that doesn't meet values specified in **Request for Comments** (**RFC**) *7230*. This can help the attacker hide the encoding of their payload from the WAF.

- **What is the difference between vertical and horizontal privilege escalation?**

  Horizontal privilege escalation refers to bypassing the authentication mechanism for users that have the same level of privilege and taking over their accounts. Vertical privilege escalation refers to escalating privilege to a higher level of access, such as a standard user now having the same level of access as the administrator account.

- **How often should organizations have an external pentest performed?**

  This answer depends on their compliance requirements, but generally, this should happen at least once a year and preferably on a quarterly basis. One thing you will notice when you're working as a pentester is that many companies will not fix any of the issues you report, so you might come back a year later and identify the same issues.

- **What are the legal considerations for pentests?**

  For pentests, you need to have a contract in place before starting the engagement. The contract is often referred to as your *get-out-of-jail-free card*, but keep in mind that you could still be arrested for performing a pentest even if it's authorized.

  Some other key legal considerations are outlined here:

  - Does the client really own the systems and/or applications they want you to test?
  - Will the client assume liability for any interruptions or damage that occur as a result of the pentest, or are you responsible?
  - What happens when third-party data or services are damaged as a result of the pentest? Who is responsible?
  - Do you need a private investigator license to perform a pentest?
  - Which jurisdiction will be recognized for the pentest? For example, if you are testing offices in Alabama and Virginia, which state's laws will apply to the engagement?
  - Who owns any new methods or tools that are developed as a result of the pentest engagement?
  - Is there a duty to warn third parties about pentest results based on the findings? For example, you discover a high-severity zero-day exploit as a result of a pentest. Do you report it?

- **Which common vulnerabilities can you exploit in pentests?**

  This can include things such as default or weak credentials, credential reuse (credential stuffing attacks), security misconfigurations (this happens a lot with cloud environments), poor patch management practices, and social engineering of the organization's staff. When I worked as a pentester, I found that I had greater success in engagements by targeting the human element (*layer 8*) than focusing on the technical side.

- **What is a buffer overflow attack?**

  Buffers are memory storage regions that temporarily hold data while it is being transferred from one location to another. A buffer overflow occurs when the volume of data exceeds the storage capacity of the memory buffer. As a result, the program attempting to write the data to the buffer overwrites adjacent memory locations.

  For example, a buffer for login credentials may be designed to expect username and password inputs of 8 bytes, so if a transaction involves an input of 10 bytes (that is, 2 bytes more than expected), the program may write the excess data past the buffer boundary.

As you can see, the questions you might be asked during an interview for pentester roles can vary, but the main thing to keep in mind is that for more junior-level roles, the interview is typically focused on knowledge with a small hands-on component. For more senior-level interviews, you can expect a more hands-on interview.

Summary

In this chapter, you learned what a pentester is, the average salaries in the US for pentesting, and common questions you might be asked during an interview. It's important to remember that the questions listed in this chapter cover entry-level through principal pentester roles, so you might not be asked all questions from this chapter during your job interview.

In the next chapter, we will learn about malware analyst careers.