Hello everyone,

Hi, I'm Bikram Kharal, a cybersecurity enthusiast and penetration tester with a strong interest in ethical hacking, network security, and offensive security. My journey into cybersecurity started with curiosity about how systems work and how they can be broken, which eventually grew into a passion for protecting them.

Over time, I've worked on sharpening my skills in penetration testing. I enjoy diving deep into real-world challenges, CTFs, and lab environments that push me to think outside the box.

I have recently given a (Offensive Security Certified Professional)OSCP/OSCP+ certification exam from Offensive Security. The OSCP is renowned for its "Try Harder" philosophy, so I knew going into the process that it would not be simple, but I learned more than just about exploitation. It taught me how to think like a hacker, to continue learning under pressure, and to persevere through difficult times.

Why I Choose OSCP certification

Having already earned certifications like CRTP, eWPTXv2, and BSCP, which are practical, hands-on exams, I sought a credential that would further challenge my skills and align with real-world penetration testing. The Offensive Security Certified Professional (OSCP) stood out as the ideal choice due to its rigorous, practical approach and strong industry reputation. Unlike certifications focused on theoretical knowledge or multiple-choice questions, the OSCP immerses you in a dynamic penetration testing environment. It requires you to actively exploit vulnerabilities, escalate privileges, and thoroughly document your findings—mirroring the demands of real-world engagements. This hands-on, challenging experience was exactly what I was looking for to advance my expertise.

My Journey of Preparation

I took a methodical approach:

PWK Labs & Course

I began by taking the Penetration Testing with Kali Linux (PWK) course offered by Offensive Security. I gained a solid foundation in information gathering, Web exploitation, privilege escalation, attacking active directory and report writing thanks to the materials. I spent hours counting, testing, failing, and trying again until I got that sweet root shell. The labs were a treasure trove.

PROF

I highly recommend going through all the lab materials and working on as many machines as possible. Crush all the labs and challenges. You may skip the challenge labs that are outside of the scope of the exam.

Practice Beyond Labs

To push myself further, I practiced on platforms like HackTheBox,PG Grounds, TryHackMe, and VulnHub. This helped me adapt to different environments and reinforced techniques I learned in the labs.

I systematically worked through the OSCP-like machines listed in the Lainkusanagi OSCP-Like Machines list to simulate real exam scenarios.

To master privilege escalation, I studied techniques from TCM Security's courses, which provided practical, in-depth insights.

For a deeper understanding of methodologies and approaches, I watched IppSec's videos, which offered valuable walkthroughs and explanations.

Additionally, I built and attacked OSCP-like Active Directory labs using Derron C's playlist to strengthen my skills in tackling complex AD environments.

Taking notes and documenting

I made it a habit to record every aspect of my preparation, including commands, screenshots, and methods for escalation of privileges. I was able to save valuable time during the exam by quickly consulting my notes thanks to this practice. I used Notion for Note taking. You can also use tools like CherryTree, Obsidian, and even basic Markdown files.

Mindset

The OSCP certification is a significant mental challenge in addition to a test of technical proficiency. I had many frustrating nights trying to get a foothold, but I learned to keep my cool, go over the enumeration steps again, and keep trying different strategies. The "Try Harder" philosophy became deeply embedded in my thinking, motivating me to overcome challenges and achieve success.

Exam Day Experience

The OSCP exam was an intense 24-hour challenge where effective time management was critical. I began by targeting machines I felt confident about, which allowed me to secure points early before moving on to the more difficult ones. Taking short breaks, eating properly, and resting briefly helped me maintain focus throughout the marathon.

The true test wasn't solely about achieving root access but maintaining consistency under pressure. By the end of the exam, I had accumulated 80 points which were enough points to pass, but the greatest sense of relief came after submitting the penetration test report. Crafting a professional, detailed report was just as crucial as compromising the machines themselves.

PROF

I started with Active Directory network. I was able to comprise the domain admmin within 5 hours. This gave me confident as I have already obtained 40 points.

After that i moved onto Linux machines, which was a easy machine i guess. I have already faced similar suitation during the preparation. I got a user and root shell within the 1 hour.

With only 10 points needed to pass, I felt optimistic but faced challenges with the final two machines. After 4 hours of enumeration without gaining initial access, stress began to mount. I took a short break, refocused, and resumed enumeration. This persistence paid off when I secured a user shell. Determined to go further, I pursued privilege escalation and ultimately achieved a root shell.

Since I still had some time left, I reviewed all my notes and screenshots one more time before finally getting some rest.

Lessons Learned

Lessons Learned

Enumeration is Key: Increase your enumeration efforts to uncover hidden vulnerabilities and pathways when progress stalls.

Keep Yourself Organized: Detailed notes and screenshots are very helpful for maintaining focus and speed during tests.

Don’t Panic Under Pressure: Approach problems methodically by dividing them into small, achievable steps to ensure consistent progress.

Balance Theory with Practice: Absorb theoretical concepts, gain a deep understanding, and immediately apply them through hands-on experimentation.

Thank you all for reading till end.