CASE STUDY

NESSUS USER PROFILES

CYBERSECURITY EDUCATION PROGRAMS FACULTY AND STUDENTS

Students in cybersecurity education programs are invaluable to this highly specialized field. They will be the next generation of bug hunters, penetration testers, consultants and chief information security officers (CISOs).

To better ensure the well-roundedness of their education, these programs typically include a class – or at least a considerable portion of one – on vulnerability assessment (VA) and/or vulnerability management (VM). In many instances, professors leading these courses turn to Nessus as a foundational tool.

Key responsibilities

Instructors in this field must conclude each semester of these advanced classes with the confidence that they have taught students the fundamentals of VA and VM. They devise lesson plans that include lab work and case studies centered around uncovering the vulnerabilities within precisely simulated fictitious organizations or real companies.

Major areas of concentration within such classes include:

- Developing a plan to identify vulnerabilities and risk within the organization
- Leveraging a synthesized mix of academic knowledge and VA tools to execute a risk assessment
- Demonstrating effective use of VA and VM solutions (plus any related software).
- Real-time response to unexpected changes in a network during a scan.
- Craft and presentation of risk assessment reports.
- Risk remediation and mitigation.

Common challenges

Students learning the fundamentals of cybersecurity must put in hard work and considerable ingenuity to meet their educational goals. Meanwhile, educators must ensure that students are in the best possible environment to absorb curriculum content and hone their skills. Without the right tools, this can be difficult.

For example, if students aren't using an effective and up-to-date vulnerability assessment solution, they won't necessarily be able to uncover all major cyberthreats or discover new vulnerabilities. If the VA software is up to date but has a notably complex or non-intuitive user interface, students might make mistakes they otherwise wouldn't while attempting to complete various tasks. In either case, these infosec-experts-in-training also likely won't be as well-equipped to learn how to adjust their scanning practices for different business environments.

If students aren't using an effective and up-to-date vulnerability assessment solution, they won't necessarily be able to uncover all major cyberthreats or discover new vulnerabilities.

How Nessus helps

Nessus didn't become the world's No. 1 vulnerability assessment solution solely because of its remarkable depth and accuracy. The software is designed with ease of use and mind, which is especially important in an educational context. Instructors can also be assured that when students use Nessus, they're working with the same vulnerability assessment tool used by professional pen testers and other cybersecurity experts in both the private and public sectors.

When students uncover vulnerabilities, Nessus will quickly rank the risk level of each hazard that is relevant to the specific organization and offer recommendations for remediation. The solution's reporting capabilities are also ideal for the classroom: Students can prepare customized reports for their instructors to review or as executive summaries for organizational leaders in real-world learning situations.

To learn more, go to www.tenable.com/tenable-for-education

Ready to get started?

TRY NESSUS FREE FOR 7 DAYS

tenable®