CASE STUDY

NESSUS USER PROFILES

THE NETWORK PEN TESTER

Network penetration testers play a unique role in the IT security ecosystem: As their primary duty is to simulate the effects of various cyberattacks on a given network, they are obligated to imagine the mindset of hackers, state-sponsored cyberattackers and other unauthorized intruders. It's not unlike the manner in which elite law enforcement agents try to think like the criminals they're pursuing.

Professional pen testers find vulnerabilities in network and computer systems, demonstrate the exploits those weaknesses might cause and aid organizations in mitigating or eliminating the flaws in question. Using Nessus, the world's No. 1 vulnerability assessment tool, can help make these cybersecurity specialists' jobs much easier.

Key responsibilities

The primary responsibility of a pen tester is to carry out penetration tests and attempt to gain system access that administrators haven't authorized them to have. This may be done remotely or on site. To successfully "intrude," it may be necessary for pen testers to develop custom scripts, worms, rootkits or other malware.

Other notable elements of a pen tester's job include:

- Assessing how flaws could affect the organization or elements of its operations.
- Creating reports on testing and breach simulations, with details on each operation, the security vulnerabilities uncovered and the levels of risk they represent.
- Making recommendations regarding the remediation and elimination of uncovered threats and explaining the adverse consequences of ignoring risk.
- Presenting executive summaries of their findings to director-level or C-suite figures within the company.

Common challenges

While it's possible that a client might have brought in a pen tester for the cybersecurity equivalent of a routine check-up, more often than not there's the strong suspicion that serious vulnerabilities exist within a system. As such, they're operating with great urgency and need to quickly assess the network areas and assets they'll be infiltrating.

But if some of the pen tester's tools aren't high-quality and lack the depth necessary to find key penetration vectors, it will be difficult to properly gauge the difficulty of the operation they're about to undertake. As a result, the tester may not be able to discover the extent of their client's risk. Lacking a cutting-edge vulnerability assessment solution also prevents testers from matching asset inventory and patch status to published vulnerabilities.

Lacking a cutting-edge vulnerability assessment solution also prevents testers from matching asset inventory and patch status to published vulnerabilities.

How Nessus helps

Leveraging the unparalleled accuracy and coverage of Nessus to conduct comprehensive vulnerability scans before breach simulations begin allows pen testers to identify the areas in need of closest examination. Scans can be carried out using prefigured policies or configured to meet custom needs.

Additionally, the Live Results feature will run an assessment with every plugin update, and can further inform a pen tester's strategy as new vulnerabilities are announced. Scan findings can quickly be turned into exported reports for IT and other stakeholders to examine, so that they're always aware of the organization's level of risk.

Nessus is also fully portable, which allows the pen tester to easily move from locations or testing sites with relative ease.

Ready to get started?

TRY NESSUS FREE FOR 7 DAYS

tenable®