USE CASE

IOACTIVE TACKLES MAJOR CYBERSECURITY OBSTACLES WITH NESSUS

Nessus is a critical element of any seasoned cybersecurity expert's toolbox, and Associate Principal Security Consultant Josep Pi Rodriguez of IOActive is no exception. Versatility, accuracy, depth and ease of use are all notable qualities of Nessus that Rodriguez has brought to bear when operating in a security consultant capacity more than a decade ago.

The dangerous illusion of invulnerability

Rodriguez credited Nessus as a critical tool in one of the biggest cybersecurity challenges he has ever faced: In fact, it was his first consulting assignment with IOActive.

"I was working for this big company in Spain, and my boss had told me no one else was able to compromise or find a critical vulnerability in this client's network," Rodriguez explained. "They were testing me, and I was under a lot of pressure."

> "I was working for this big company in Spain, and my boss had told me no one else was able to compromise or find a critical vulnerability in this client's network, they were testing me, and I was under a lot of pressure."
>
> **Josep Pi Rodriguez**
>
> Associate Principal Security
> Consultant of IOActive

Finding the vulnerability needle in the network haystack

Because the company had several of its key IP addresses exposed to the internet, Rodriguez was all but certain that there was a crack in the company's network armor – regardless of how fruitless others' searches had been. He first enumerated all of the client's IP addresses and then used Nessus to scan for potential threats. Nearly all had no issues. But Nessus noted the presence of a recent zero-day vulnerability in a service that was listening on the port of a single IP address. Rodriguez was then able to reverse-engineer his own exploit and remotely compromise the company's entire internal network, proving that it was not the flawless environment it appeared to be on the surface.

"Nessus had a small role in this story, but to me it's a critical one," Rodriguez said. "Because back then I had limited time for this engagement, and thanks to Nessus I was able to find the only vulnerable service in hundreds of IP addresses."

> "Nessus had a small role in this story, but to me it's a critical one, because back then I had limited time for this engagement, and thanks to Nessus I was able to find the only vulnerable service in hundreds of IP addresses."
>
> **Josep Pi Rodriguez**
> Associate Principal Security Consultant of IOActive

The value of reliability

Rodriguez noted that Nessus' ability to find vulnerabilities in situations where hundreds or even thousands of IP addresses needed to be scanned had been extremely useful to him throughout his career. He also took the time to note that the solution had always been easy to use and stood out considerably among its competitors.

"I can remember testing other, similar products, both paid and free ones, and based on my experience Nessus has always been the best," Rodriguez said. "Not only in terms of its findings but also speed and stability. And when I've talked with other consultants and [cybersecurity] colleagues, they agree with me."

tenable