Open source intelligence (OSINT) has long been a valuable commodity to ethical penetration testers and malicious hackers alike, but recent high-profile attacks and breaches has moved OSINT even further into the spotlight. This talk will quickly introduce the typical steps followed during a penetration test and the goals of such an engagement. We will then focus on how OSINT about the target organization is gathered, the value of OSINT in each step of the penetration test, and how openly available information can ultimately bring down even the most security-conscious organizations.