

Username: Palm Beach State College IP Holder **Book:** Kali Linux – Assuring Security by Penetration Testing. No part of any chapter or book may be reproduced or transmitted in any form by any means without the prior written permission for reprints and excerpts from the publisher of the book or chapter. Redistribution or other use that violates the fair use privilege under U.S. copyright laws (see 17 USC107) or that otherwise violates these Terms of Service is strictly prohibited. Violators will be prosecuted to the full extent of U.S. Federal and Massachusetts laws.

Summary

In this chapter, we discussed the target enumeration process and its purpose. We also discussed port scanning as one of the target enumeration methods. You learned about several types of port scanning, and then we looked at several tools, such as Nmap, [Unicornsca](#)n , and [Amap](#) . Next, we talked about SMB enumeration using [nbtscan](#) and SNMP enumeration using [onesixtyone](#) and [snmpcheck](#) . Lastly, we talked about VPN enumeration and [ike-scan](#) as the tool to carry out this process.

In next chapter, we will look at vulnerability identification, a process of identifying and analyzing the critical security flaws in the target environment.