

Security Tools

Lab 10

ITSC 200: Network Protocols and Security

Table of Contents

[Lab Outcome(s) 2](#_Toc465173395)

[Reading 2](#_Toc465173396)

[Introduction 2](#_Toc465173397)

1. [Installing Kali Linux and using Nmap, Etherape, netcat 3](#_Toc465173398)

[References 4](#_Toc465173400)

Lab Outcome(s)

* Install Kali Linux and use nmap, Etherape, and netcat.
* Review a Wireshark capture of nmap and netcat.

Reading

* None

Introduction

This lab is to practice the installation of Kali Linux in a virtual machine and the use, and installation of some basic security tools. It also looks at a detailed capture of a nmap scan and a netcat connection.

1. Installing Kali Linux  
   1. Create a new virtual machine in Virtualbox  
      1. Set the Operating System type to “Debian 64” (Kali is based on Debian Linux)
      2. Set RAM to 4 GB.
      3. Set the networking to NAT (for now).
      4. Set the disk space to dynamic and 40 GB.
      5. Attach the Kali ISO to the virtual CDROM
   2. Start the VM.
   3. Once the install is complete, check the IP address, subnet mask, DNS, and default gateway.
   4. Log into your new Kali VM as root with the password you assigned during the install.
   5. Find Zenmap and prepare a couple of scans of your home network. You may see your cell phones, game consoles, smart TV, and other devices on your network.
   6. Write down the command as it appears in Zenmap.
   7. Nmap one of the devices on your home network. What ports are open ?
   8. If you have another computer on your network, run Wireshark to see what the nmap scan looks like.
   9. Make sure you try it at the command line. With a remote connection it is unlikely that you will have a GUI.
   10. Run Etherape on your home network and watch the connections that your computer makes. Some of the connections are likely to surprise you.
   11. Try to use netcat to copy a file from one computer to another over a high port (if you have another computer).
   12. Think about some ways that netcat could be used by employees in your company (the most frequent source of security breaches) to compromise your company’s network.

Lab submission : For each of these tools (Nmap, Etherape, and Netcat) suggest how they could be helpful in doing a penetration test of a network. Submit your review to the Lab 10 OS Assignment folder on D2L.

References

[https://nmap.org](https://nmap.org/)

<http://nc110.sourceforge.net/>

<https://www.sans.org/security-resources/sec560/netcat_cheat_sheet_v1.pdf>

<https://nmap.org/ncat/> - This is a different version of netcat called ncat. Along with having some interesting features, you can download a version for Windows.

Blank page if necessary to make pages an even number

**DO NOT DELETE THE SECTION BREAK BELOW. DELETING IT MAY IMPACT THE FORMATTING IN THIS DOCUMENT.**