

Lab 10

Security Tools

ITSC 200: Network Protocols and Security

Table of Contents

[Lab Outcomes 4](#_Toc490651418)

[Reading 4](#_Toc490651419)

[Introduction 4](#_Toc490651420)

[1.0 Installing Kali Linux 5](#_Toc490651421)

[References 7](#_Toc490651422)

Lab Outcomes

* Install Kali Linux and use Nmap, driftnet and Netcat.
* Review a Wireshark capture of Nmap and Netcat.

Reading

* None

Introduction

This lab gives you practice in 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 an Nmap scan and a Netcat connection.

1. Installing Kali Linux
2. 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.
3. Start the VM.
4. Once the install is complete, check the IP address, subnet mask, DNS and default gateway.
5. Log in to your new Kali VM as root with the password you assigned during the install.
6. Find Zenmap and prepare a couple of scans of the network and your classmates’ laptops.
7. Write down the command as it appears in Zenmap.

1. Nmap each other’s laptops with the firewall running and with the firewall down.

1. If you are the nmap’ee, then run Wireshark to see what it looks like.
2. Make sure you try it at the command line. With a remote connection it is unlikely that you will have a GUI.
3. Do some research and use Nmap to try to find the IP address of the printer in the room (5,000 guru points to the first person to do this).
4. Try to use Netcat to copy a file from one computer to another over a high port.
5. Use Netcat to open a remote bash shell on another student’s computer.
6. Challenge: See if you can, in groups of three, copy a file from one computer, bounce it off another computer and have it end up on a third computer (10,000 guru points for the first group to do it).
7. 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.

References

<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 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.**