

Security Tools

Lab 11

ITSC 200: Network Protocols and Security

Table of Contents

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

[Reading 2](#_Toc465173396)

[Introduction 2](#_Toc465173397)

1. [Installing Port Sentry, ARPWatch, Fail2ban 3](#_Toc465173398)

[References 4](#_Toc465173400)

Lab Outcome(s)

* Install Port Sentry, ARPWatch, and Fail2ban.
* Learn how iptables displays rules.

Reading

* None

Introduction

This lab is to practice the installation of several security tools that help secure a Linux host from attackers. It also demonstrates how iptables rules are used to dynamically block unwanted traffic.

1. Installing security tools  
   1. Using the Linux Mint install that you did earlier in the course, install several tools that will help you protect your computer.
   2. Use the lecture material to help you install ARPWatch on your Linux Mint computer.
   3. After about 20 seconds, tail the /var/log/syslog file.
   4. Can you see any new MAC addresses listed ?
   5. Note that a “-f” can be used with the tail command to watch a log file and see additional entries in real time. (use ctl-c to stop it)
   6. Use the lecture material to install Fail2ban on your computer correctly.
   7. Configure it to monitor your ssh server (if you don’t have an ssh server running, go ahead and install it with “sudo apt-get install openssh-server”).
   8. From your real computer “ssh blah@<your vm ip address>” 4 or 5 times with a failed password.
   9. Were they blocked eventually ? What message did they get when they tried to ssh into your computer again ?
   10. Check your firewall (“sudo iptables –L”) to verify that their IP address was added as a firewall rule.
   11. Use the lecture material to install Port Sentry correctly.
   12. From your real computer use Nmap to port scan the IP address of the Linux Mint.
   13. Could you ping your Linux Mint computer after ?
   14. Could you connect to your Linux Mint computer on any port ?
   15. Look into the port sentry host.deny file to verify that your real computer’s IP address is listed.

**Lab Submission :** No lab submission.

References

<https://www.tecmint.com/monitor-ethernet-activity-in-linux/>

<http://www.faqs.org/docs/securing/chap14sec117.html>

<https://adamscheller.com/systems-administration/fail2ban-ssh-ubuntu-debian-mint/>

<https://www.digitalocean.com/community/tutorials/how-to-protect-ssh-with-fail2ban-on-ubuntu-14-04>

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.**