Cabrillo College

Lab 9: Embedded Operating Systems

In this lab, we will add a new Android "Lollipop" VM to play the role of the victim. We will use the Kali VM as the attacker. The attacker will create and publish a "backdoor" payload on a website. This payload appears to be a normal Google App package; however, it is not coming from a trusted location. The victim downloads and installs this file even though it does not come from the Google Play store. Once installed, the backdoor payload will connect back to the attacker. The attacker can them view and download information from the victim.

Warning and Permission

Unauthorized hacking can result in prison terms, large fines, lawsuits and being dropped from this course!

For this lab you have authorization to hack the VMs in the VLab pod assigned to you.

Preparation

- Get the CIS 76 Login Credentials document. You will need usernames and passwords to log into VLab and each of the VMs. This document is on Canvas and the link is in the CIS 76 Welcome letter.
- Determine which VLab pod number you were assigned. See the link on the left panel of the class website.

Reference Links

- The Pod Setup Guide: https://simms-teach.com/docs/cis76/cis76-podSetup.pdf
- Lesson 11: https://simms-teach.com/docs/cis76/cis76lesson11.pdf

Part 1 – Verify DHCP has been configured on your EH-pfSense VM

1) See Lesson 11.
2) Capture the DHCP settings for your report**.**

Part 2 – Setup, snapshot and test your EH-Lolli-xx VM

1) Use the Pod Setup Guide to configure your EH-Lolli VM.
2) Capture the ifconfig and ping tests for your report.

Part 3 - Obtain some data on EH-Lolli-xx

1) See Lesson 11, select any image you like.
2) Capture the File Manager view showing downloaded image file.

Part 4 - Create a "backdoor" payload on EH-Kali

1) See Lesson 11.
2) Capture the creation of the payload.

Part 5 – Make a website on EH-Kali to distribute payload

1) See Lesson 11.
2) Capture view of the malicious website.

Part 6 – Exploit Android from EH-Kali

1) See Lesson 11.
2) Capture handler setup and start of exploit.

Part 7 – On EH-Lolli install the malicious "backdoor" payload

1) See Lesson 11.
2) Capture successful installation of backdoor payload.

Part 8 – Exfiltrate the image file from EH-Lolli

1) See Lesson 11.
2) Capture download command and desktop showing image.

Submit your work

1) Prepare a report using the word processor and formatting of your choice. Your report should contain the following:

    - Course name, lab assignment name, your name, and date.
    - Part 1 [EH-pfSense-xx] DHCP configuration.
    - Part 2 [EH-Lolli-xx] ifconfig and ping test.
    - Part 3 [EH-Lolli-xx] File Manager showing downloaded image file.
    - Part 4 [EH-Kali-xx] Creating "backdoor" payload.
    - Part 5 [EH-Kali-xx] Website with malicious "backdoor" payload.

- Part 6 [EH-Kali-xx] Setup and start Metasploit exploit.
- Part 7 [EH-Lolli-xx] Successful installation of payload.
- Part 8 [EH-Kalli-xx] Exfiltrate and display stolen image file.

As an example you can see Benji Simms' report here:
https://simms-teach.com/docs/cis76/cis76-lab09-simben76.pdf

2) Email your report to: **risimms@cabrillo.edu**

Remember **late work is not accepted.** If you run out of time submit what you have completed for partial credit.

Grading Rubric (30 points)

2 points for the part 1.
4 points each for the parts 2-8.