



PRIFYSGOL CYMRU
Y Drindod Dewi Sant
UNIVERSITY OF WALES
Trinity Saint David
SWANSEA - ABERTAWE



School of
Applied Computing

Advanced Cyber Security (ACS)

Lab – Cloud Computing

**Faculty of Architecture, Computing &
Engineering
School of Applied Computing
IQ Building, Room 205
Swansea
SA1 8EW**

Cloud computing is Internet-based computing in which large groups of remote servers are networked to allow sharing of data-processing tasks, centralized data storage, and online access to computer services or resources.

Task 1: Performing Cloud Vulnerability Assessment Using Mobile-Based Security Scanner zANTI.

zANTI is a mobile penetration-testing toolkit that lets security managers assess the risk level of a network with the push of a button. This easy-to-use mobile toolkit enables IT Security Administrators to simulate an advanced attacker to identify the malicious techniques they use to compromise corporate networks.

Lab Scenario

zANTI enables Security Administrators to effectively assess an organization's system and naturally diagnose vulnerabilities in cell phones or sites utilizing a large group of infiltration tests including, man-in-the-middle (MITM), secret word splitting, and metasploit.

As a **security administrator**, you need to ensure that the website related to your organization provides encryption to the communications passing through HTTP channel.

Lab Objectives

The objective of this lab is to help students learn how to scan for vulnerabilities in cloud environment through Android Mobile Devices.

Pre- Activity exercise

To carry out the lab, you need:

- Computers running Windows
- zANTI which is located on the shared drive lecturer PC.

- You can download the latest version of zANTI from <https://www.zimperium.com/zanti-mobile-penetration-testing>
- If you decide to download the latest version, screenshots and steps might differ in your lab environment.
- Run this lab in Android as Attacker Machine
- Administrative privileges to run the tool
- A web browser with Internet access in both the machines

Overview of Lab

SSL/TLS provides communication security and privacy over the Internet for applications such as web, email, instant messaging (IM) and some virtual private networks (VPNs). Data flowing through the channel is encrypted and is difficult to decode.

Activity:

Note: Screenshot may varies from the one in this lab. Though the lab says Windows server 2008, use Windows 7 and/or Windows 10 if the Windows server 2008 is not available.

Note: Before running this lab, log in to **Windows Server 2008** and ensure that you stop IIS admin service and World Wide Web Publishing Service (if you have the service installed on the machine.). To stop the service, go to **Start → Administrative Tools → Services**, right-click **IIS Admin Service** and click **Stop**, right-click **World Wide Web Publishing Service** and click **Stop**. Also ensure that you stop Internet Information Services (IIS) Manager and Internet Information Services (IIS) 6.0 Manager. To stop Internet Information Services (IIS) Manager, go to **Start → Administrative Tools → Internet Information Services (IIS) Manager**, right-click on the server name in the left pane and click **Stop** to stop the manager. To stop Internet Information Services (IIS) 6.0 Manager, go to **Start → Administrative Tools → Internet Information Services (IIS) 6.0 Manager**, right-click on the server name in the left pane, and click **Disconnect** to disconnect the manager.

Make sure that you delete all the cookies in the browser in which you will be hosting **ownCloud** and make sure that WAMPServer is kept online throughout this lab.

1. In **Windows Server 2008**, click **Start** button at the lower-left corner of the screen, and then click **start WAMPServer** to launch WAMPServer.

2. Launch the **Android** machine from **Hyper-V Manager**, and wait until it boots. Then click Menu icon, as shown in the figure, to view installed apps.

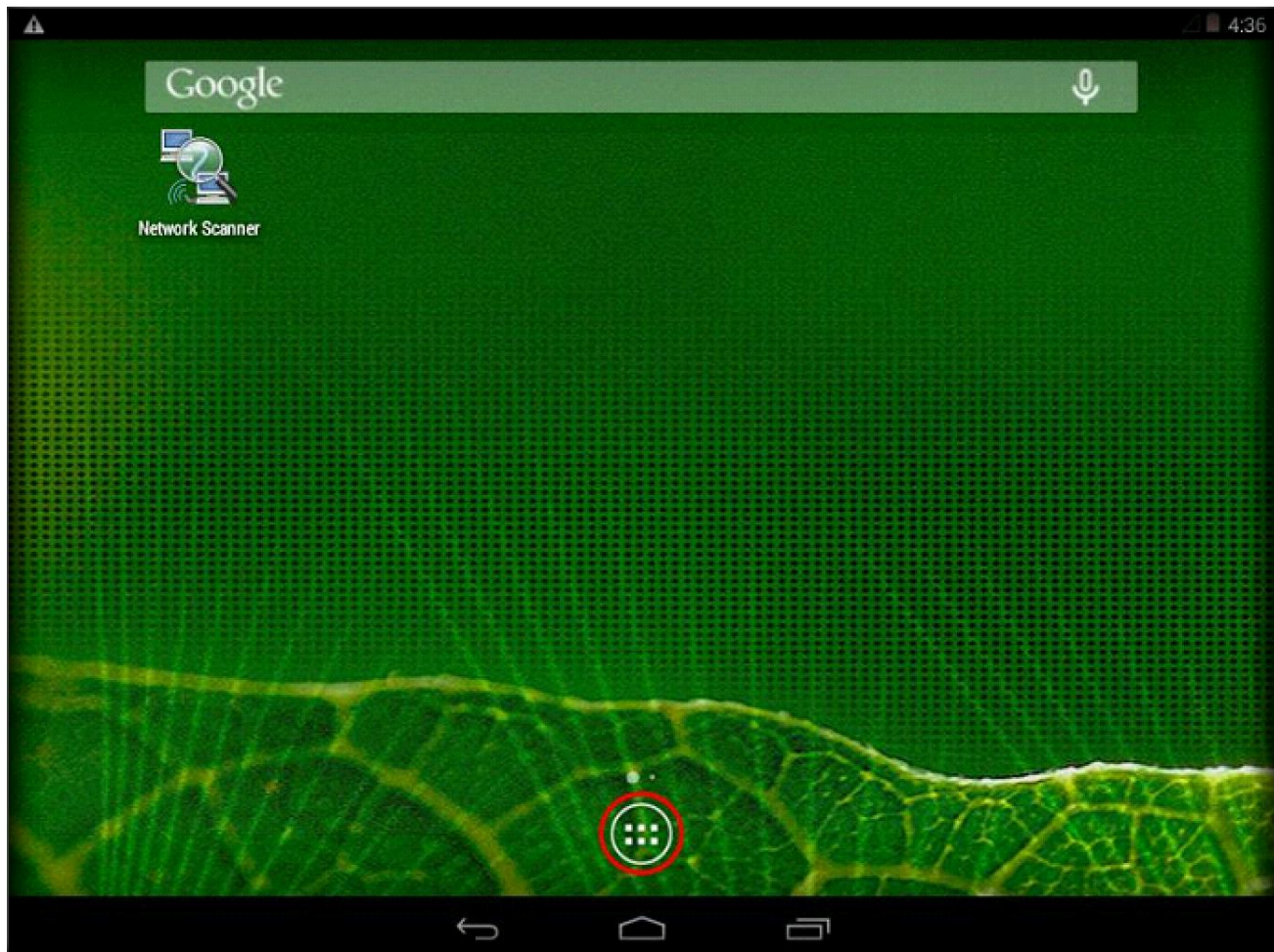


FIGURE 4.1: Android Emulator main Screen

3. Now, click **ES File Explorer** app from apps menu to access the shared folder from Windows Server 2012

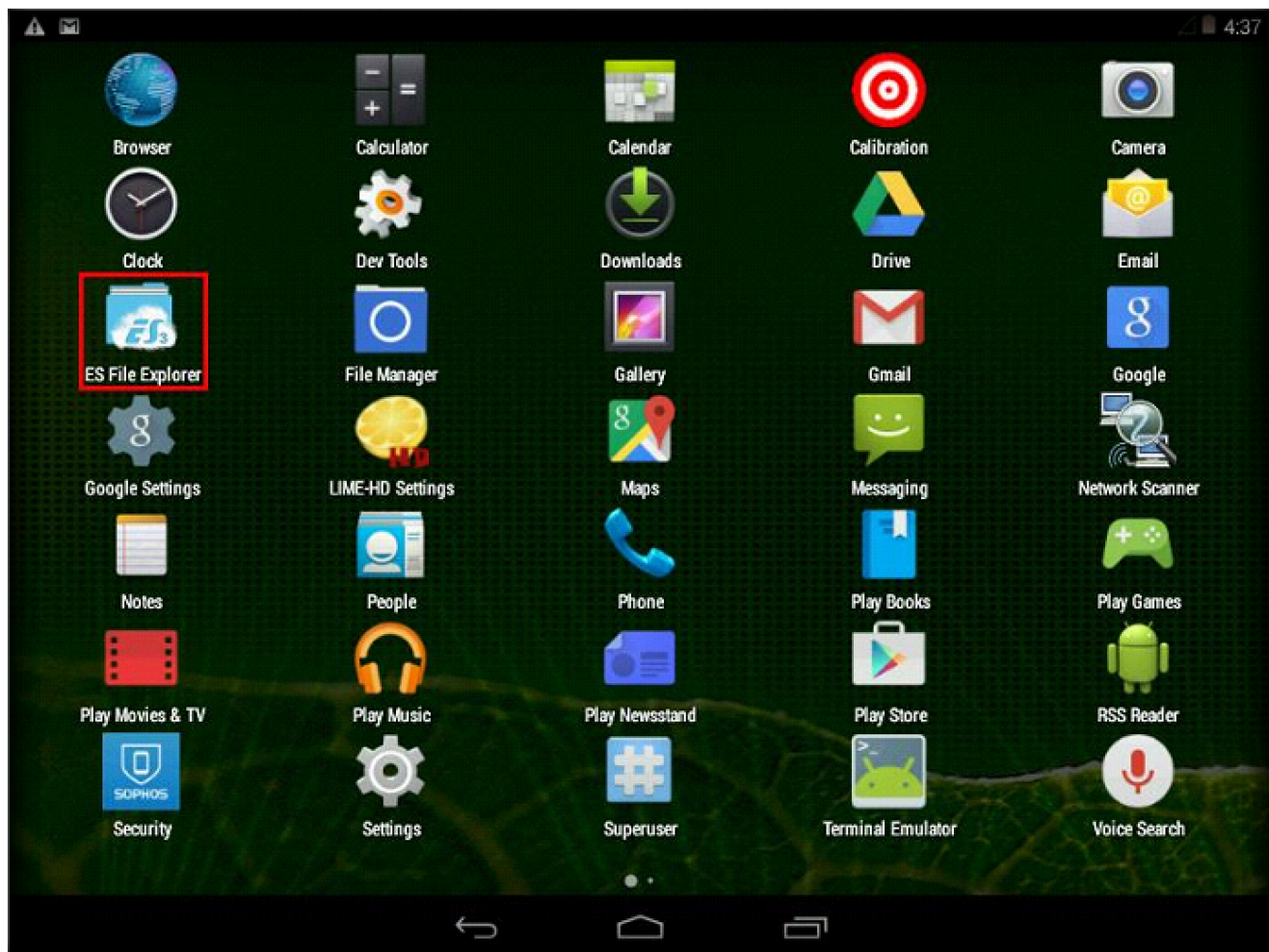


FIGURE 4.2: Android Emulator Apps Screen

4. The ES File Explorer window appears; in the left pane, click **Network** node, and click **LAN** in the menu.

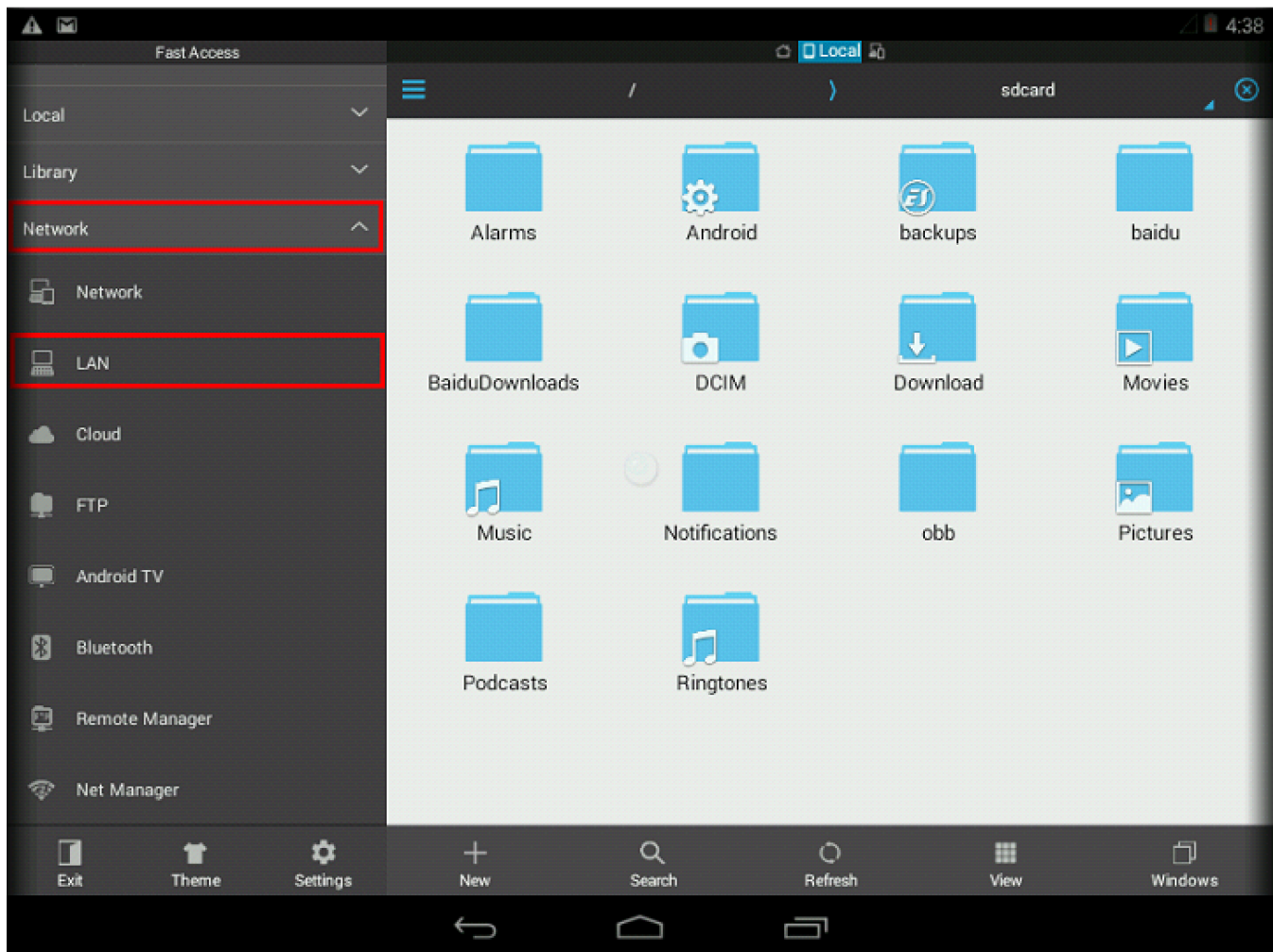


FIGURE 4.3: ES File Explorer Main Window

5. In the **LAN** window, click **New** option to connect the shared folder.

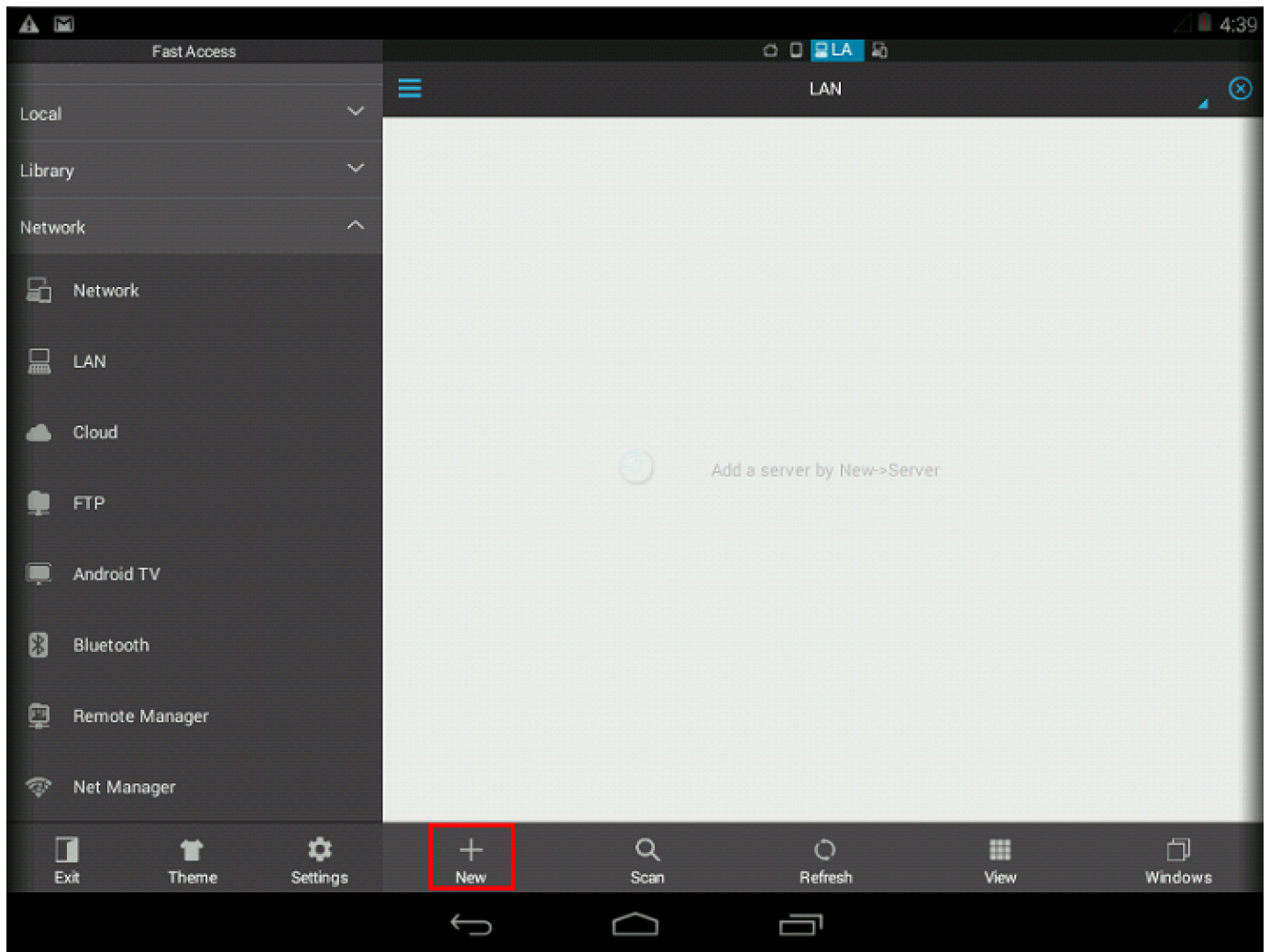


FIGURE 4.4: ES File Explorer LAN Configuration

6. Server pop-up appears, type Windows Server 2012 IP address in **Server** field and enter Windows Server 2012 credentials in the **Username** and **Password** fields, and click **OK** to continue.
7. In this lab, the IP address of the Windows Server 2012 is 10.0.0.5, which may differ in your lab environment.

Server

Domain Domain name, can be empty

Server 10.0.0.5
Example:192.168.1.100/My Documents

Username Administrator

Password

☐ Anonymous

Display as Click to edit, can be empty

Cancel OK

FIGURE 4.5: ES File Explorer Server pop-up

8. The **Windows Server 2012** machine will connect, as shown in the screenshot.
9. Click the computer icon to view the shared folders.

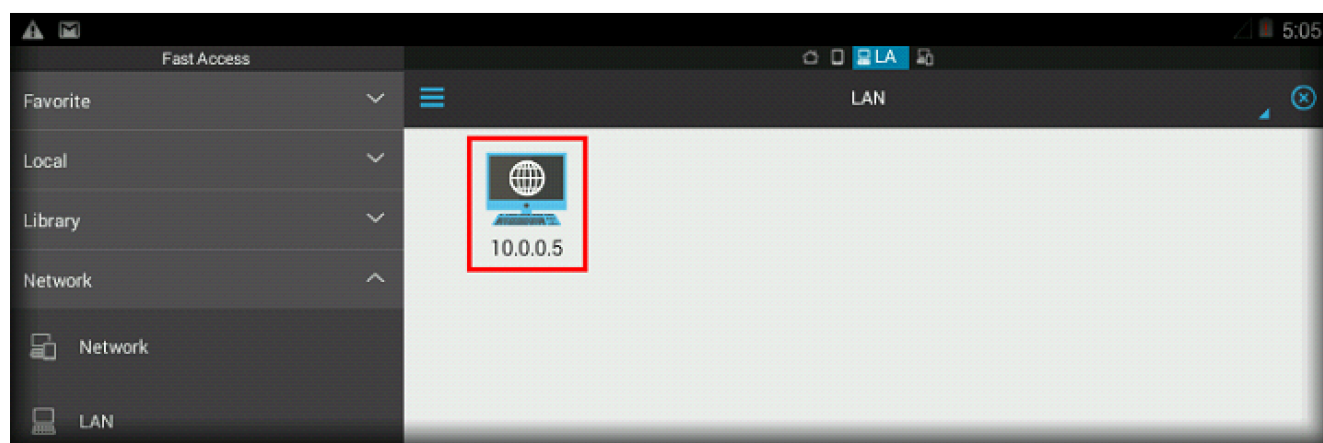


FIGURE 4.6: ES File Explorer show Windows Server 2012 Machine

10. Now, it will show you all shared folders on Windows Server 2012, click the **CEH-Tools** shared folder.

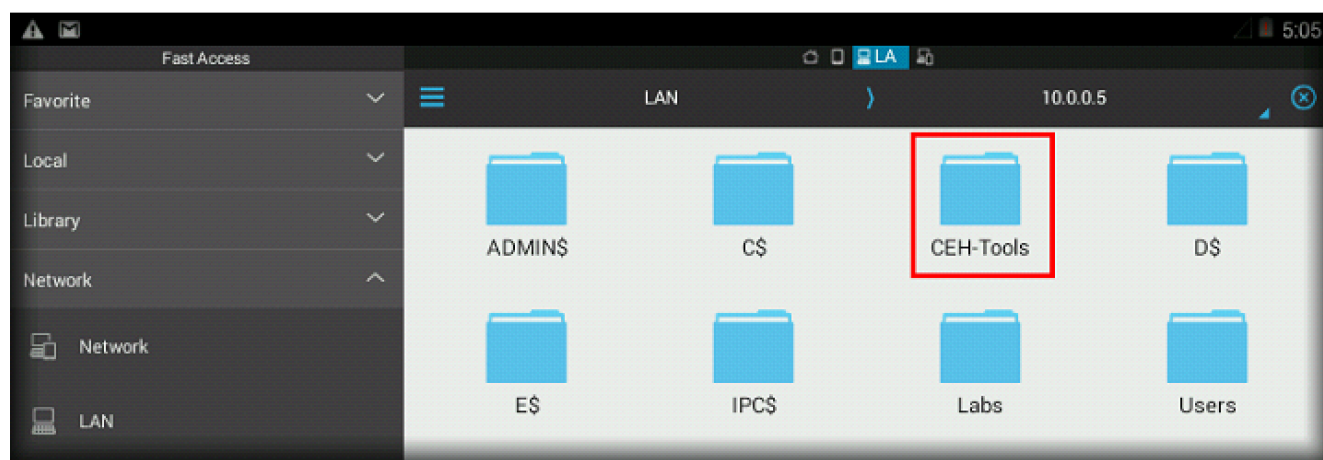


FIGURE 4.7: ES File Explorer Share CEH-Tools folder

11. Click the **CEHv9 Module 15 Hacking Mobile Platforms** folder to view the tools.

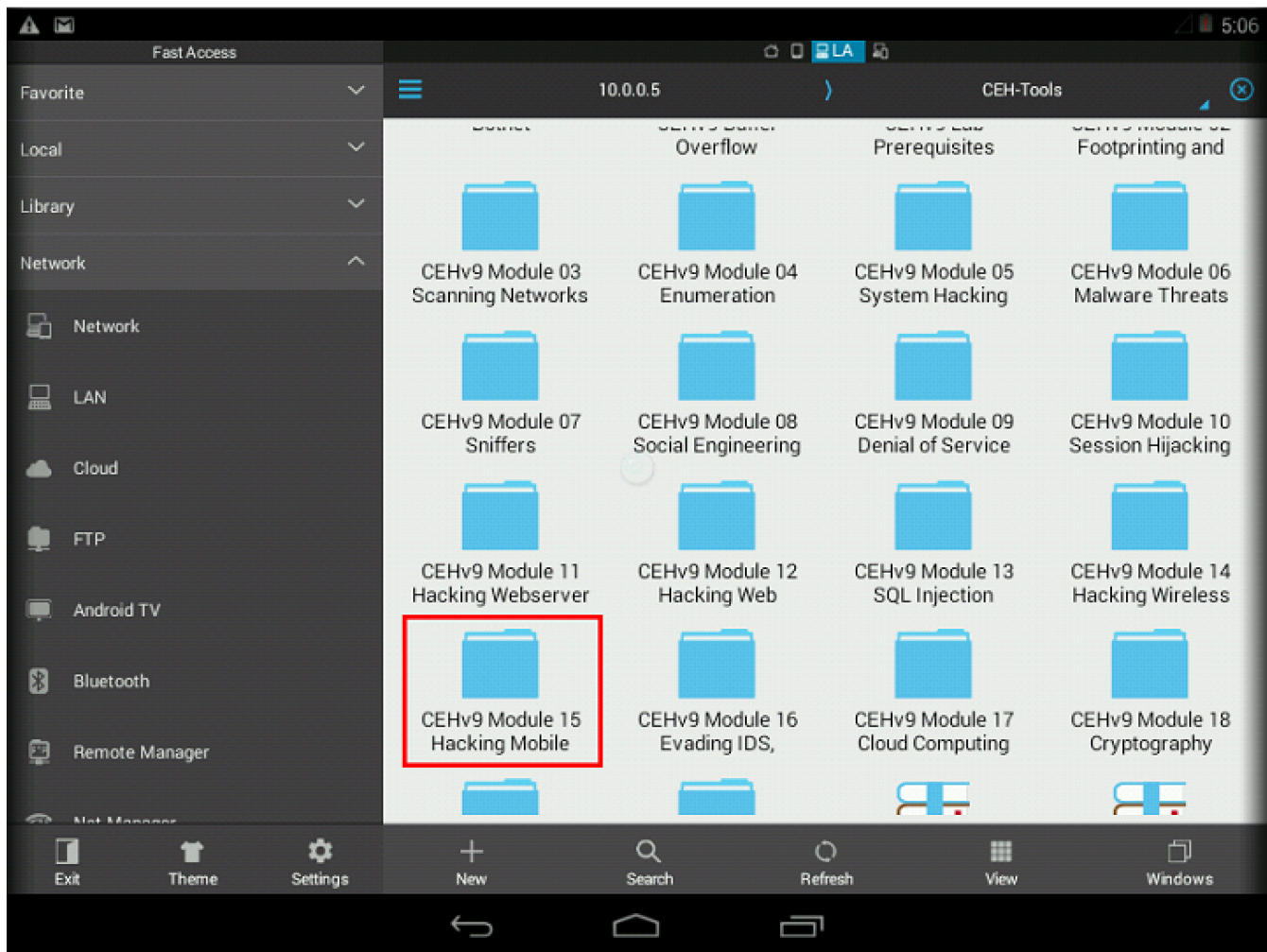


FIGURE 4.8: ES File Explorer Shared CEH-Tools

12. Click the **Mobile Pentesting Toolkit** folder.

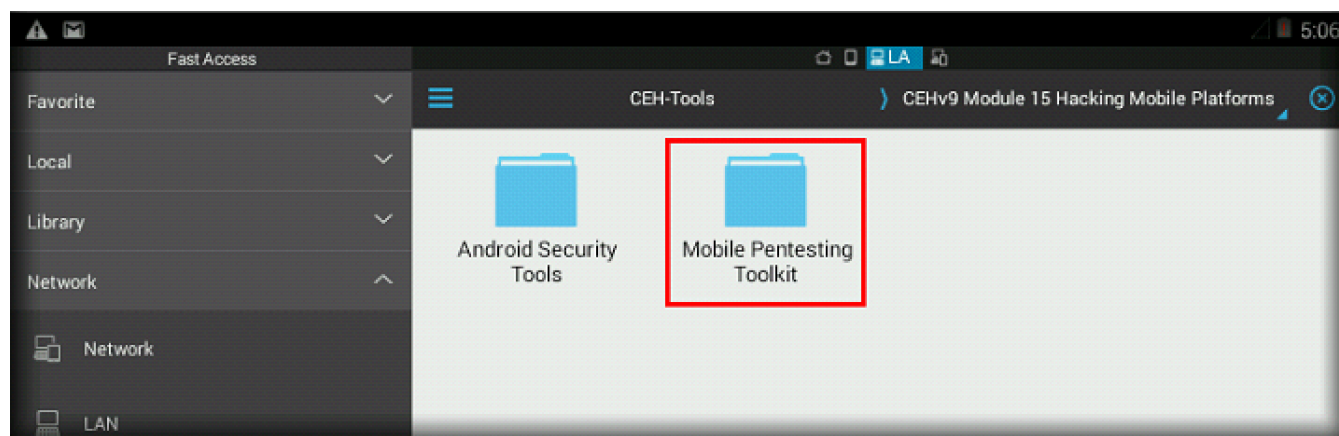


FIGURE 4.9: ES File Explorer Shared Mobile Platforms Tools

13. Click the **ZANTI** folder, and then click **zANTI2.apk** to proceed with the installation.

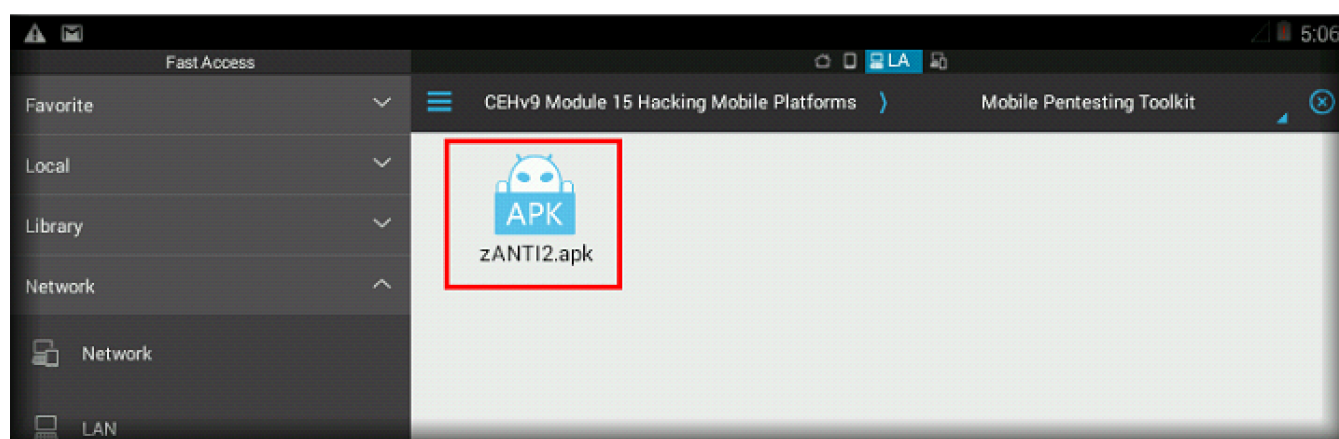


FIGURE 4.10: zANTI.apk file

14. If the properties pop-up appears, click **Install** to continue.

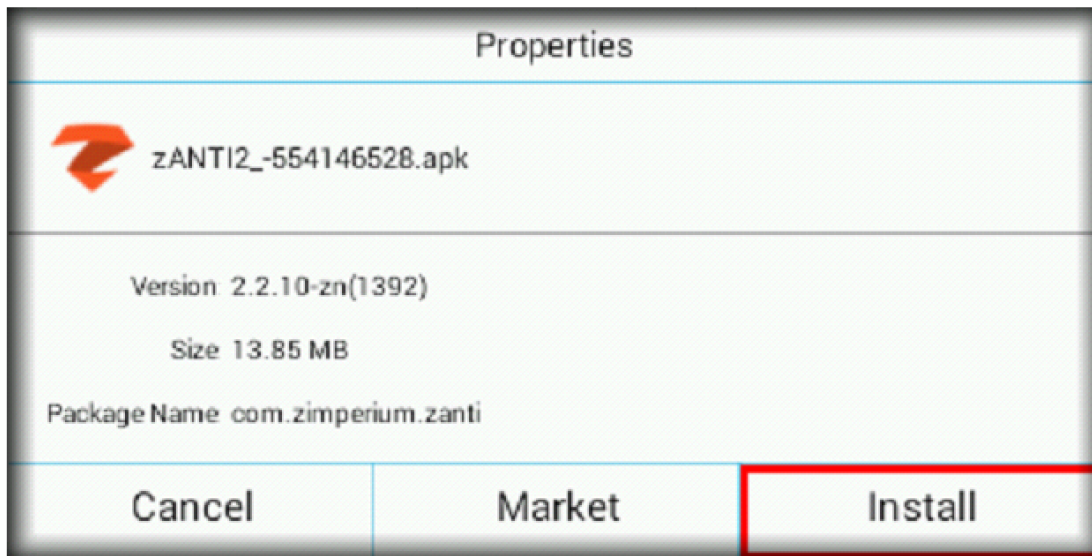


FIGURE 4.11: zANTI.apk Properties

15. The Select pop-up will ask you to choose an installer package; choose **Package Installer**.

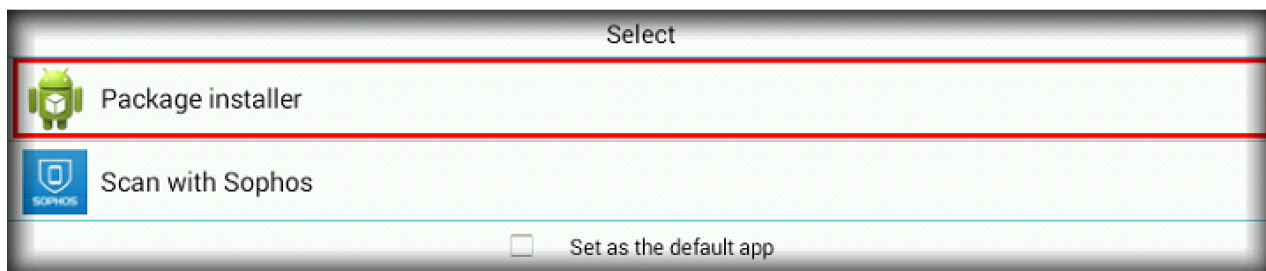


FIGURE 4.12: Choosing Installer

16. If an Android device any **Mobile Security** app is installed, the prompt **Threat Detected** displays; click **Continue**.

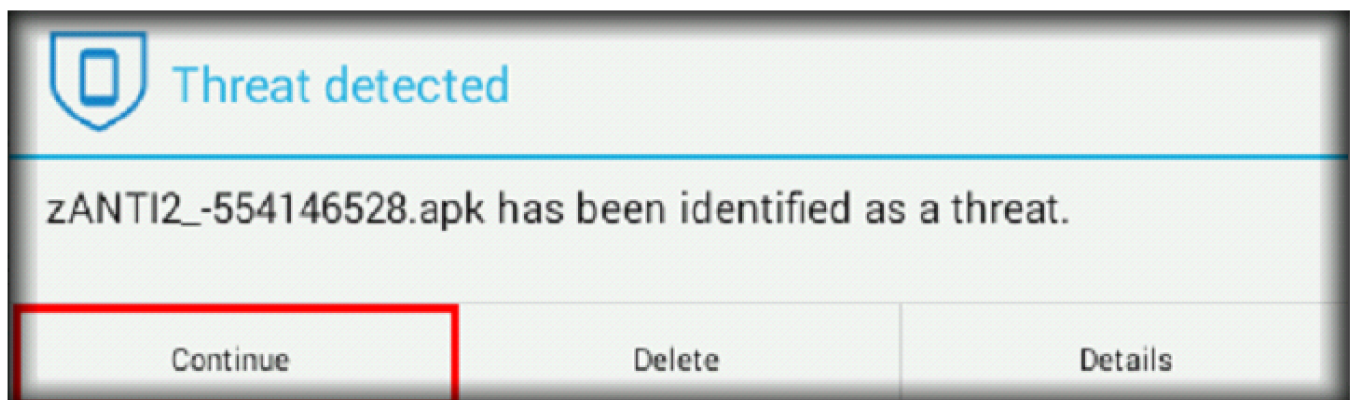


FIGURE 4.13: Threat Detected pop-up

17. The prompt **Do you want to install this application** appears; click **Next** to continue.

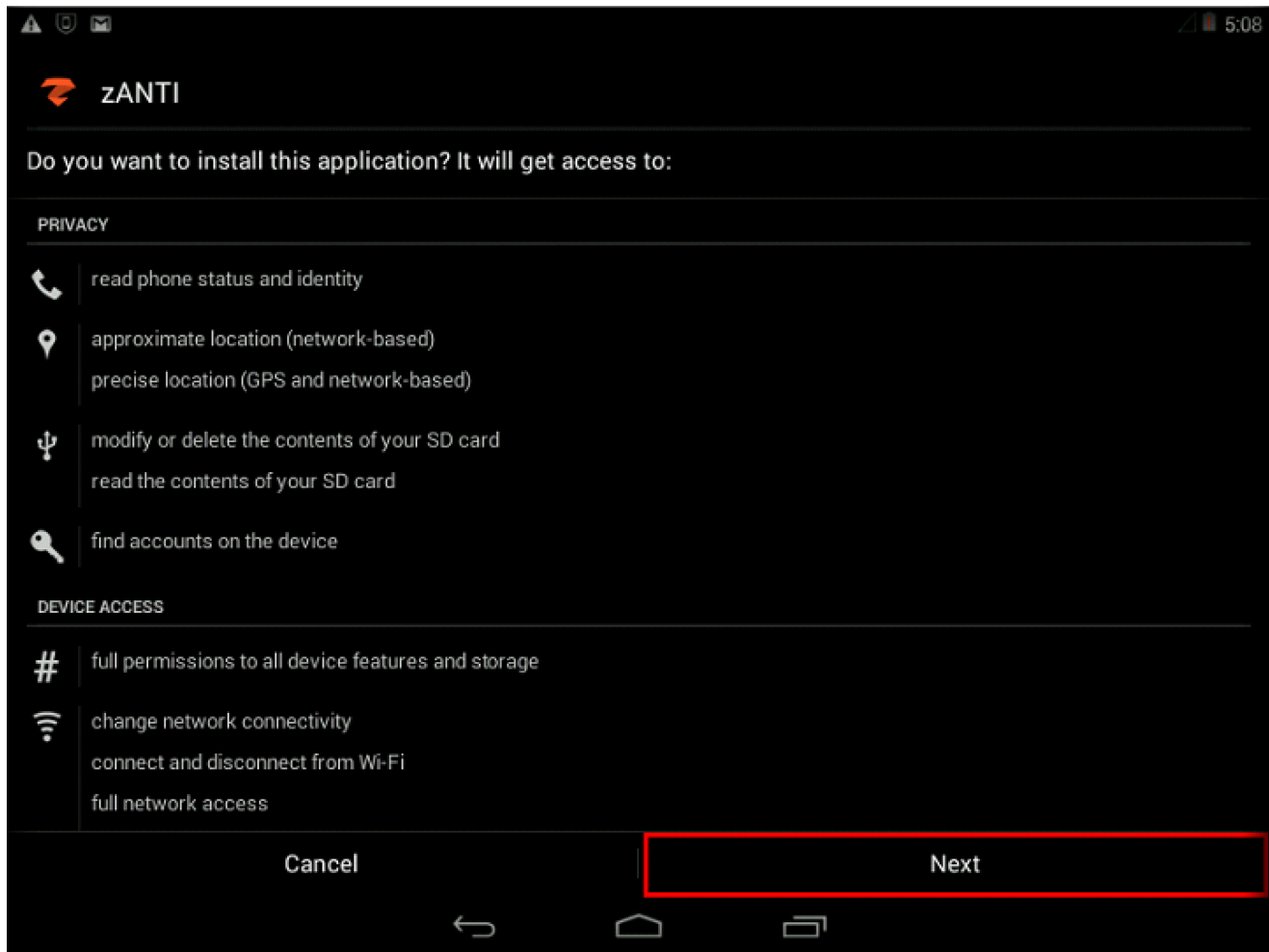


FIGURE 4.14: zANTI Installation-1

18. When the **Device Access** screen appears, click **Install**.

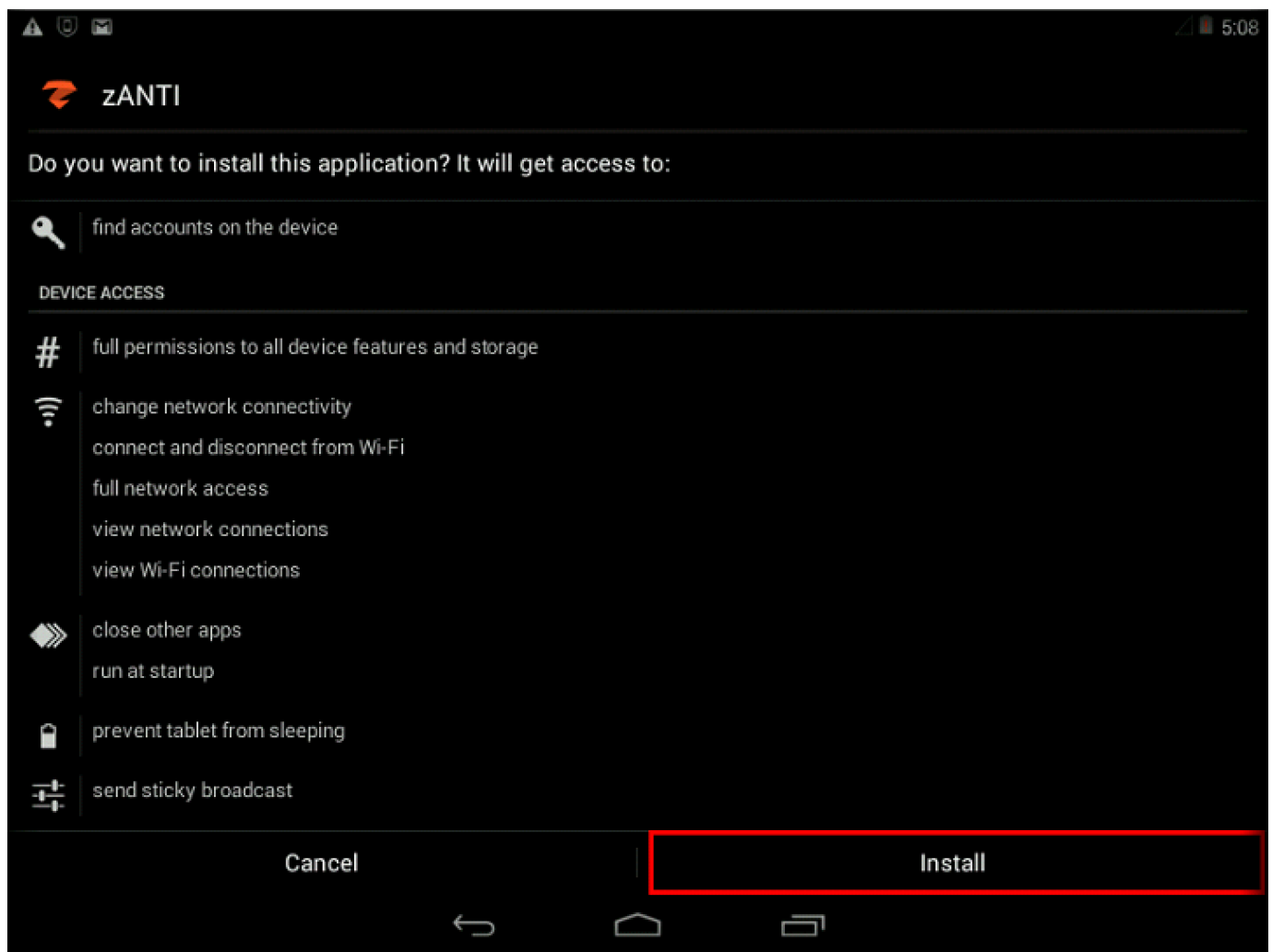


FIGURE 4.15: zANTI Installation-2

19. **zANTI** will start the Installation process, as shown in the screenshot.



FIGURE 4.16: zANTI Installation Process

20. If the **Threat detected** pop-up appears, click **Cancel** to continue.

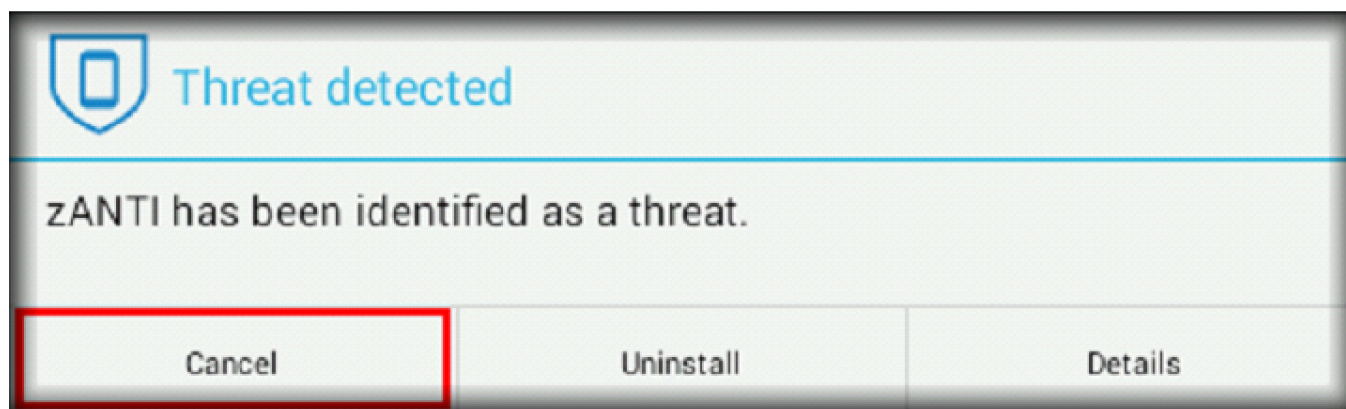


FIGURE 4.17: Threat Detected pop-up

21. Once the app is installed successfully, click **Open**.

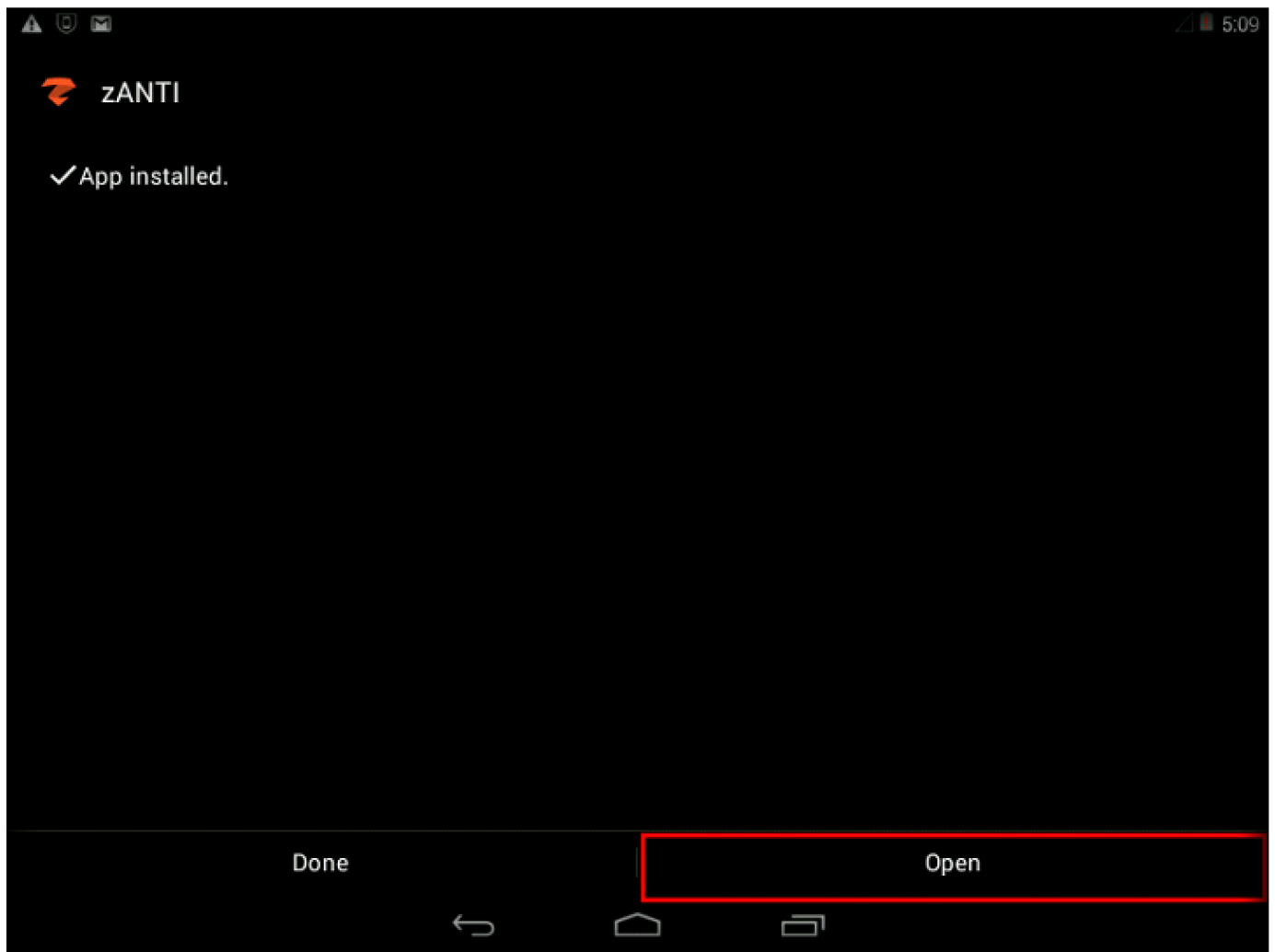


FIGURE 4.18: zANTI Successfully Installed

22. To run zANTI, the Android device requires Superuser access. If the **Superuser Request** pop-up appears, choose **Remember choice forever**, and click **Allow**.

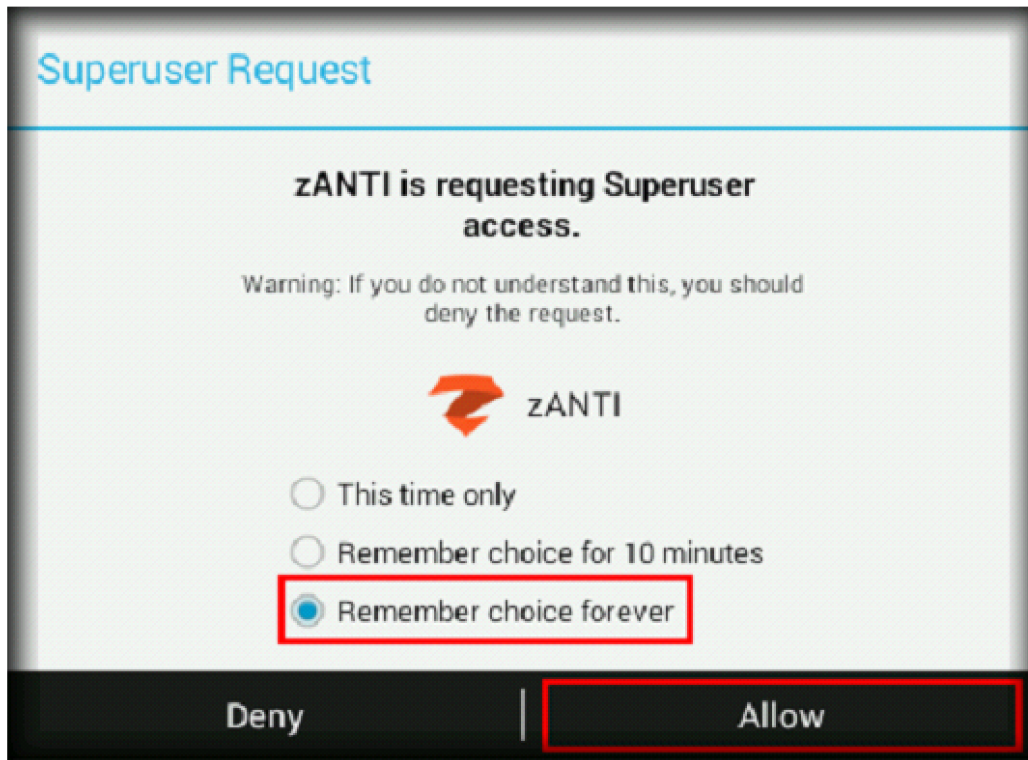


FIGURE 4.19: Superuser Request pop-up

23. If the **Threat** pop-up appears, click **Allow** to continue.

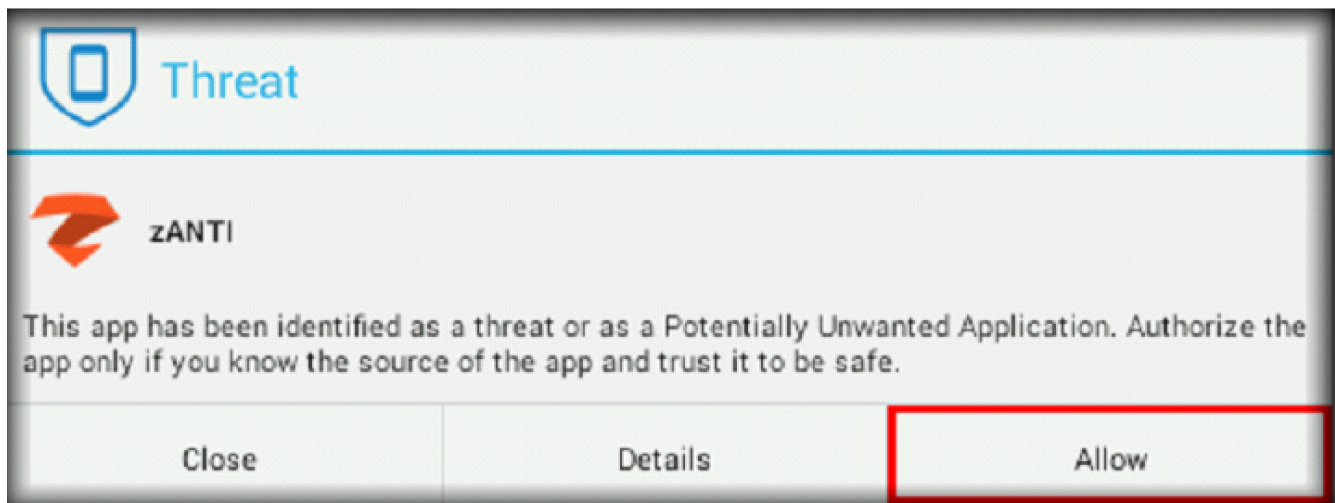


FIGURE 4.20: Threat Pop-up

24. The zANTI main screen appears in the Play Store, as shown in the screenshot, with a registered email ID.

25. Now, check **I accept Zimperium's EULA** and uncheck **Join Zimperium's Security Feed**; then click **Start Now**.

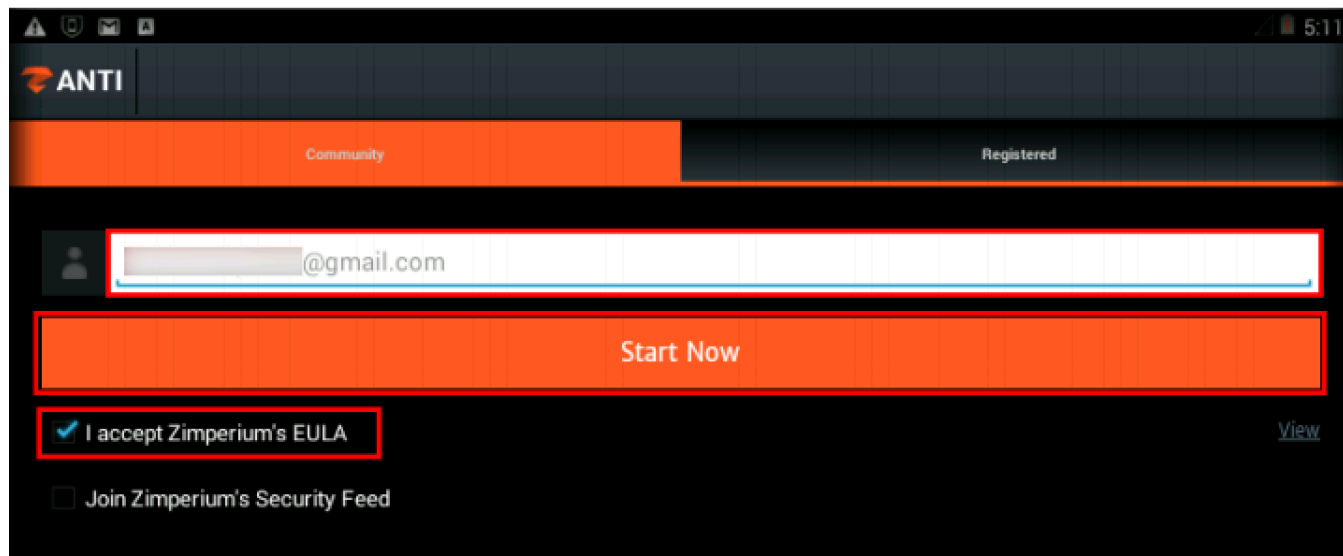


FIGURE 4.21: zANTI EULA Screen

26. The **Join the zNetwork** screen appears; click **Skip**.

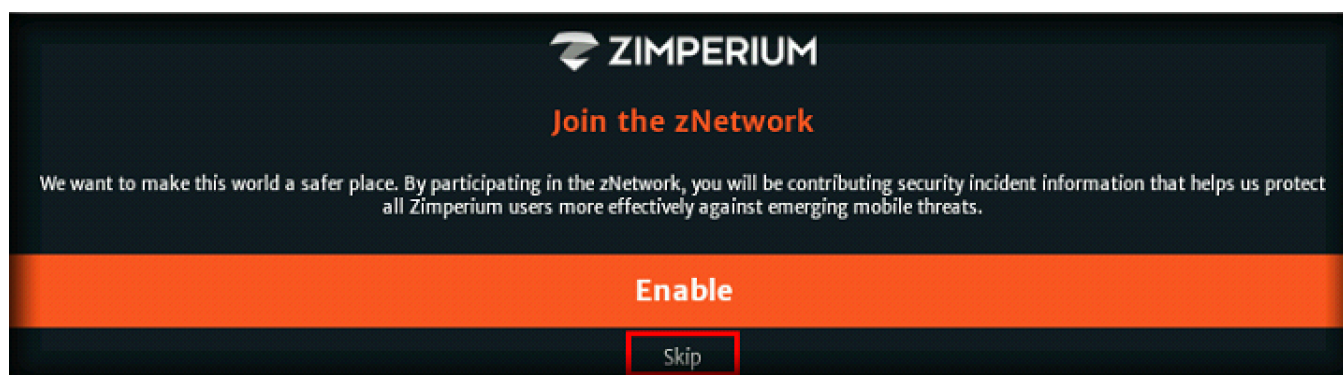


FIGURE 4.22: Join the zNetwork Screen

27. zANTI will start communicating with its servers to register. Wait until it finishes this process.

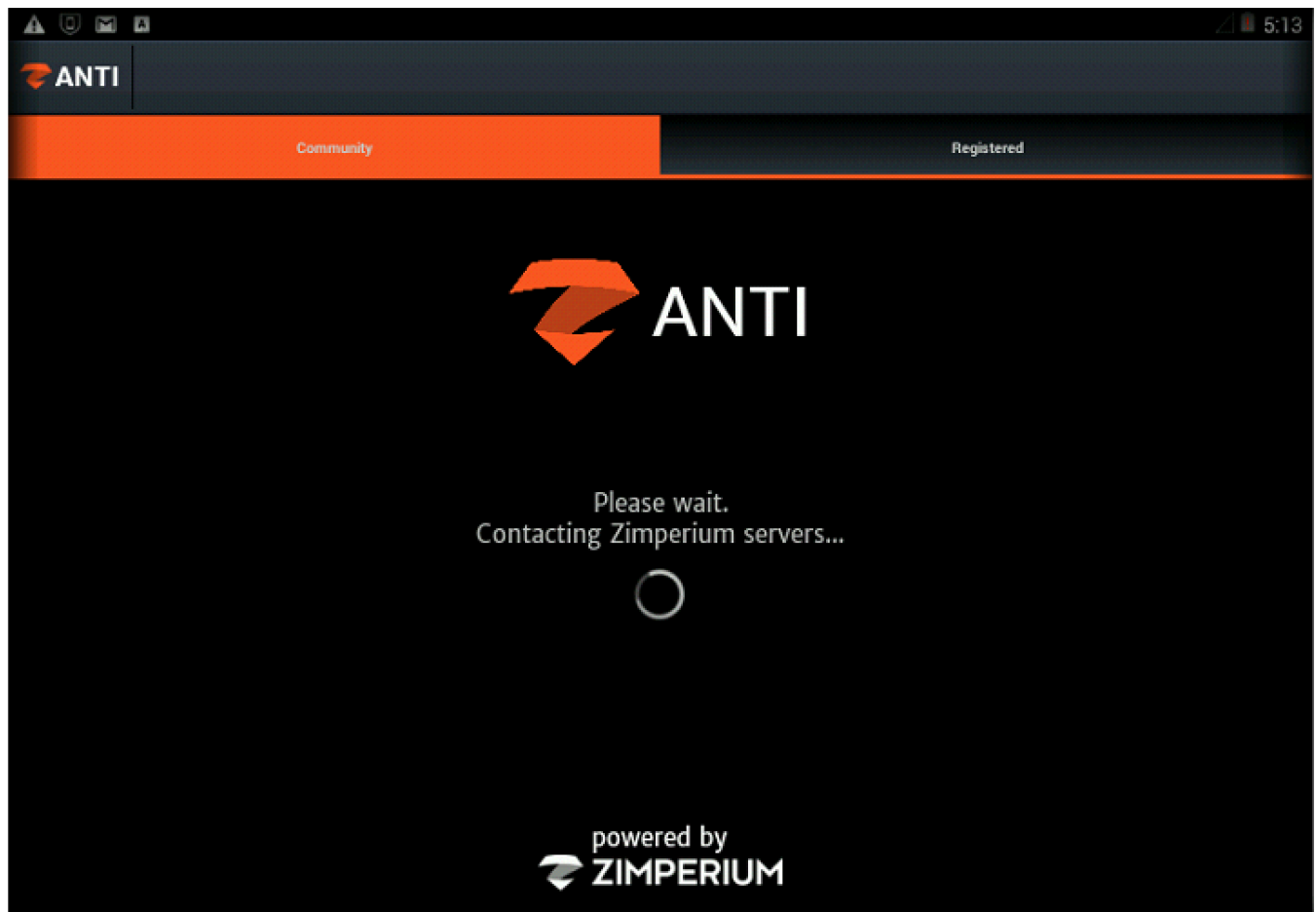


FIGURE 4.23: Contacting Zimperium Servers Screens

28. The zANTI main screen appears; click **SKIP** in the upper-right corner of the window.

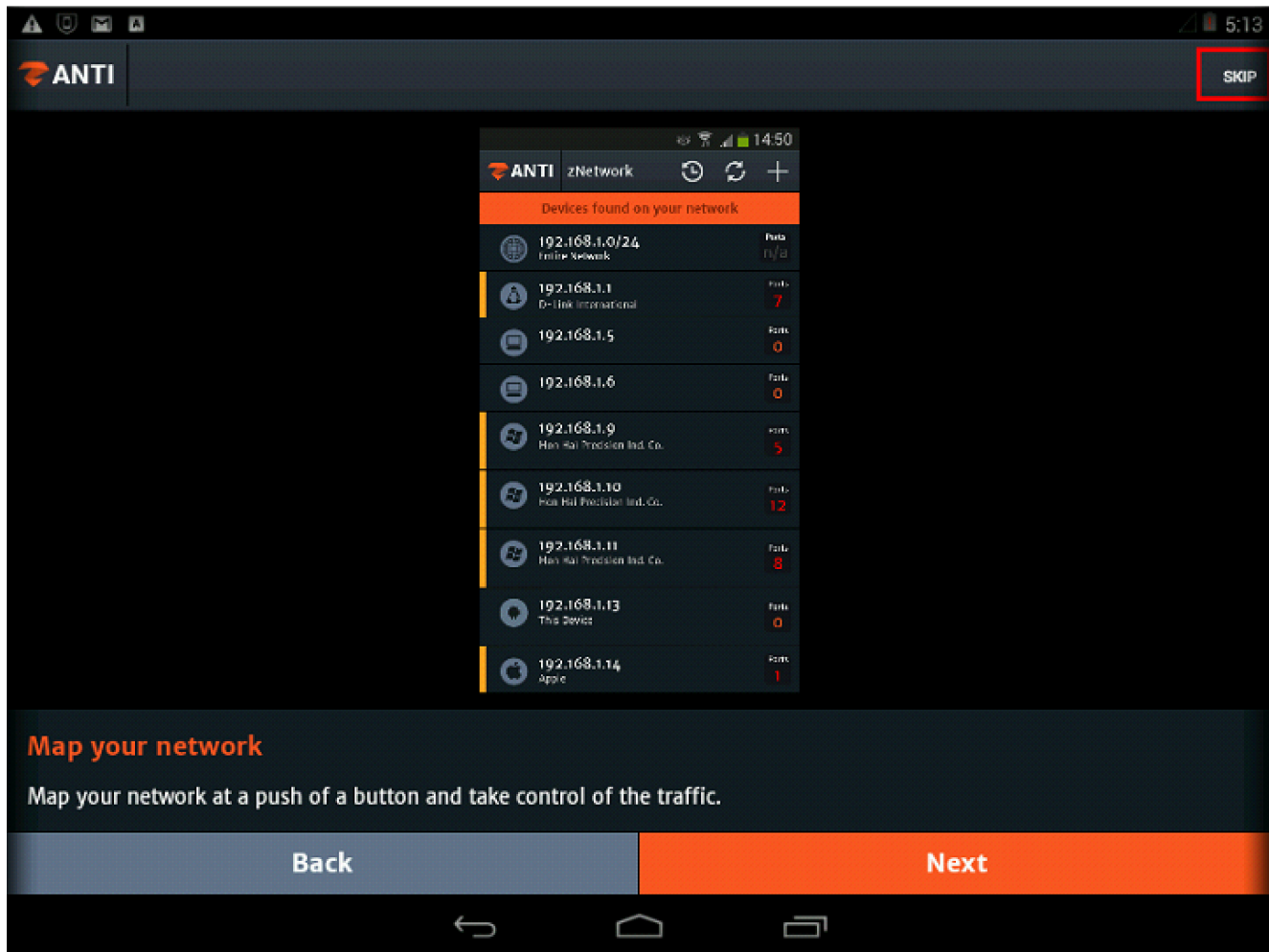


FIGURE 4.24: Map Your Network

29. Check **I am fully authorized to perform penetration testings** on the network check box, and click **Next**.

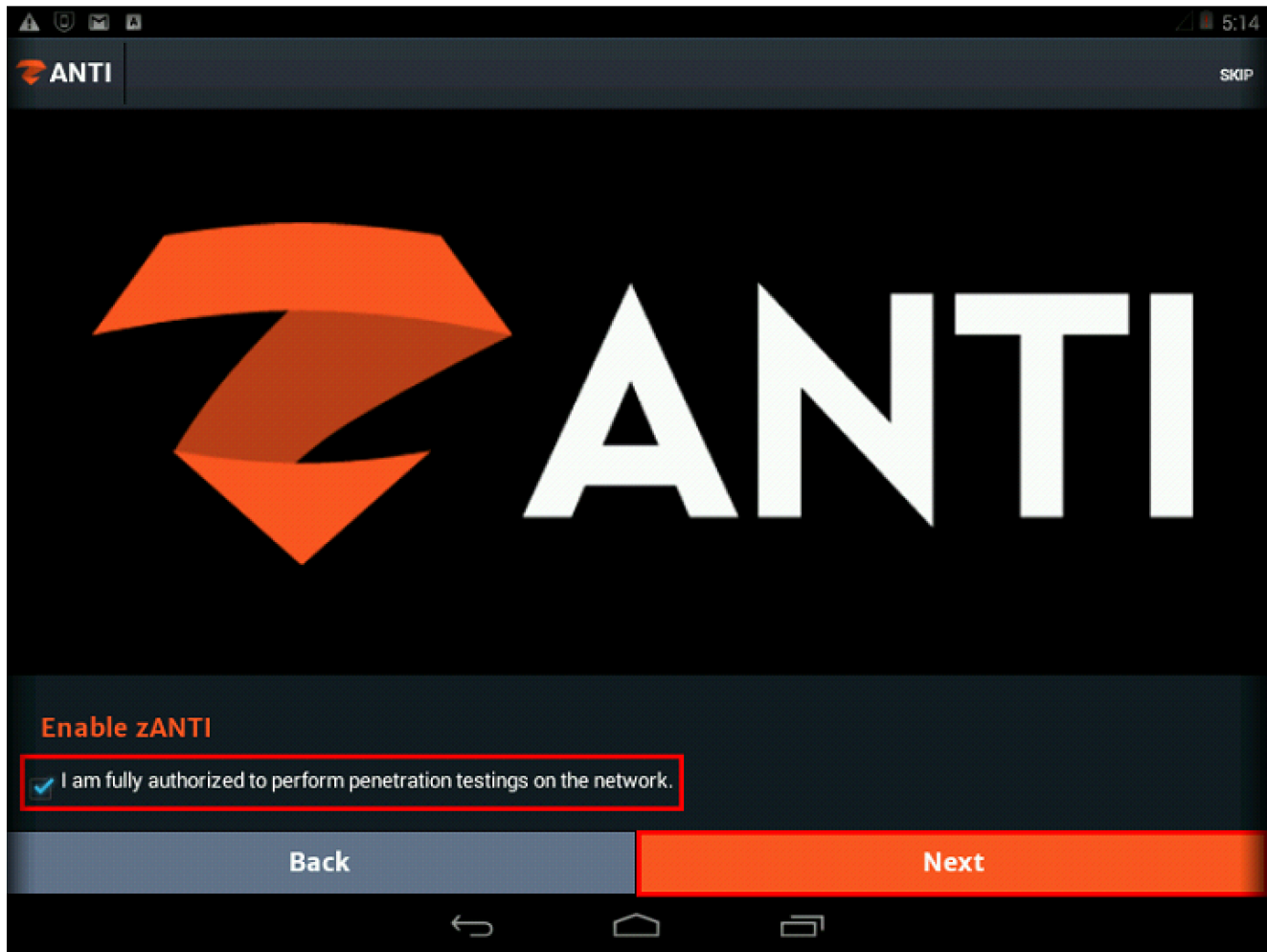


FIGURE 4.25: Enabling zANTI

30. Click **Clock** in the right side of the screen to configure **zANTI**.

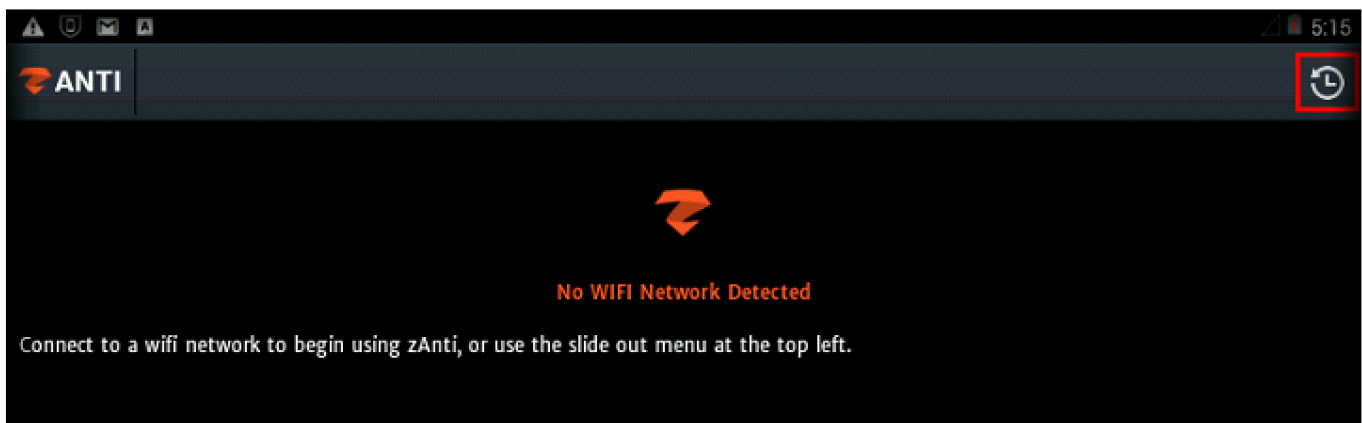


FIGURE 4.26: Configuring zANTI

31. Devices found on your network screen appears click **+** icon from right hand side screen to add or configure.

32. By default, it will displays IP addresses of Zimperium and scanme.nmap.org.

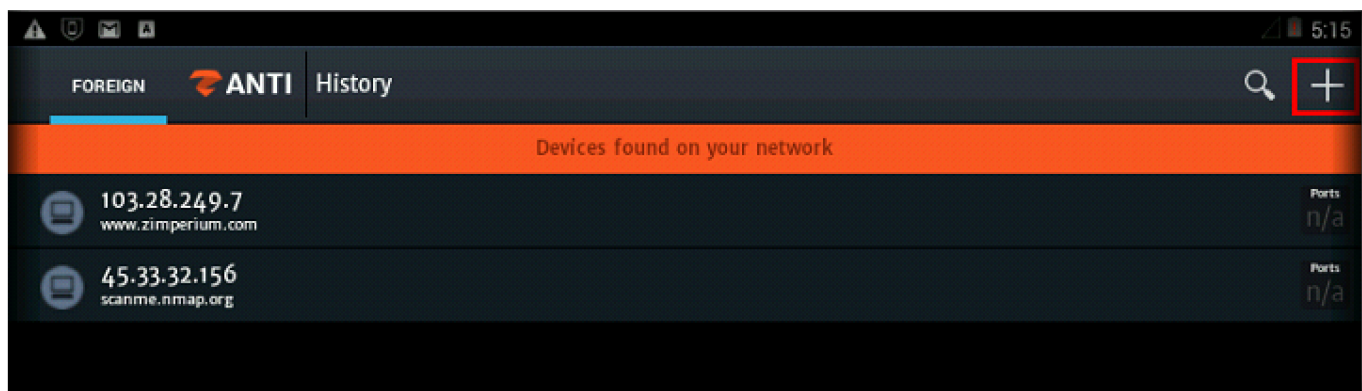


FIGURE 4.27: Adding a New Target

33. Once you click on **+** icon **Add host to Foreign** pop-up appears, type the IP address of the Windows Server 2008 machine in the field, and click **OK**.

Note: The IP address shown in this lab may differ in your lab environment.

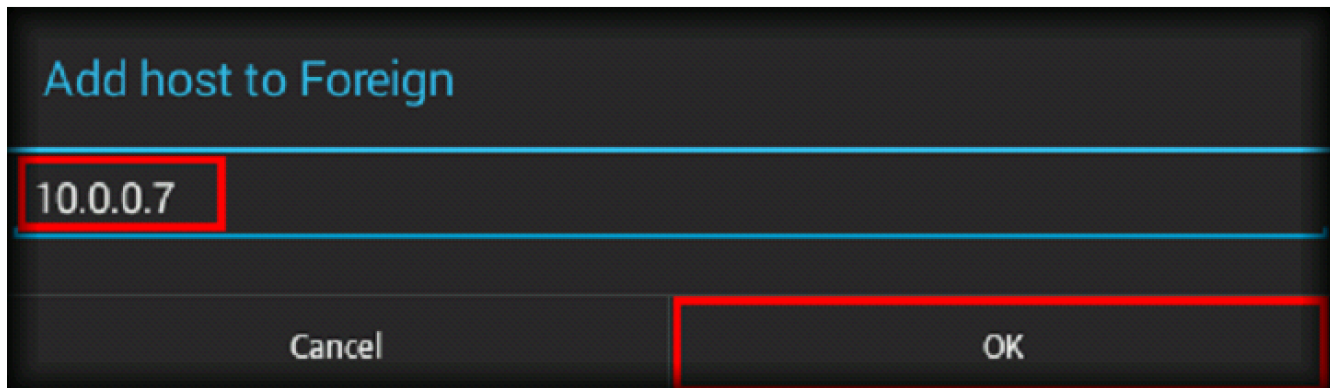


FIGURE 4.28: Add host to Foreign

34. Once the host is added in the **Devices found on your network** history, click on the added **host IP address** to proceed to the next step.

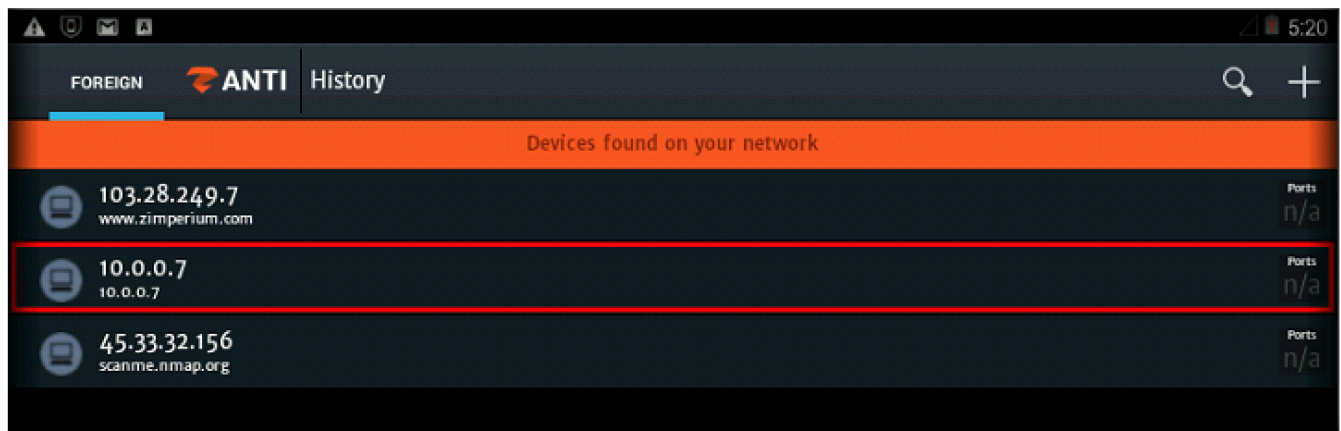


FIGURE 4.29: Added new host

35. The **zANTI target @ Added IP address of the machine** screen appears.
36. Now, perform the **Heartbleed** vulnerability scan on the target machine (i.e., Windows Server 2008).
37. To perform this scan, click **Heartbleed** (under **Attack Options**), as shown below.

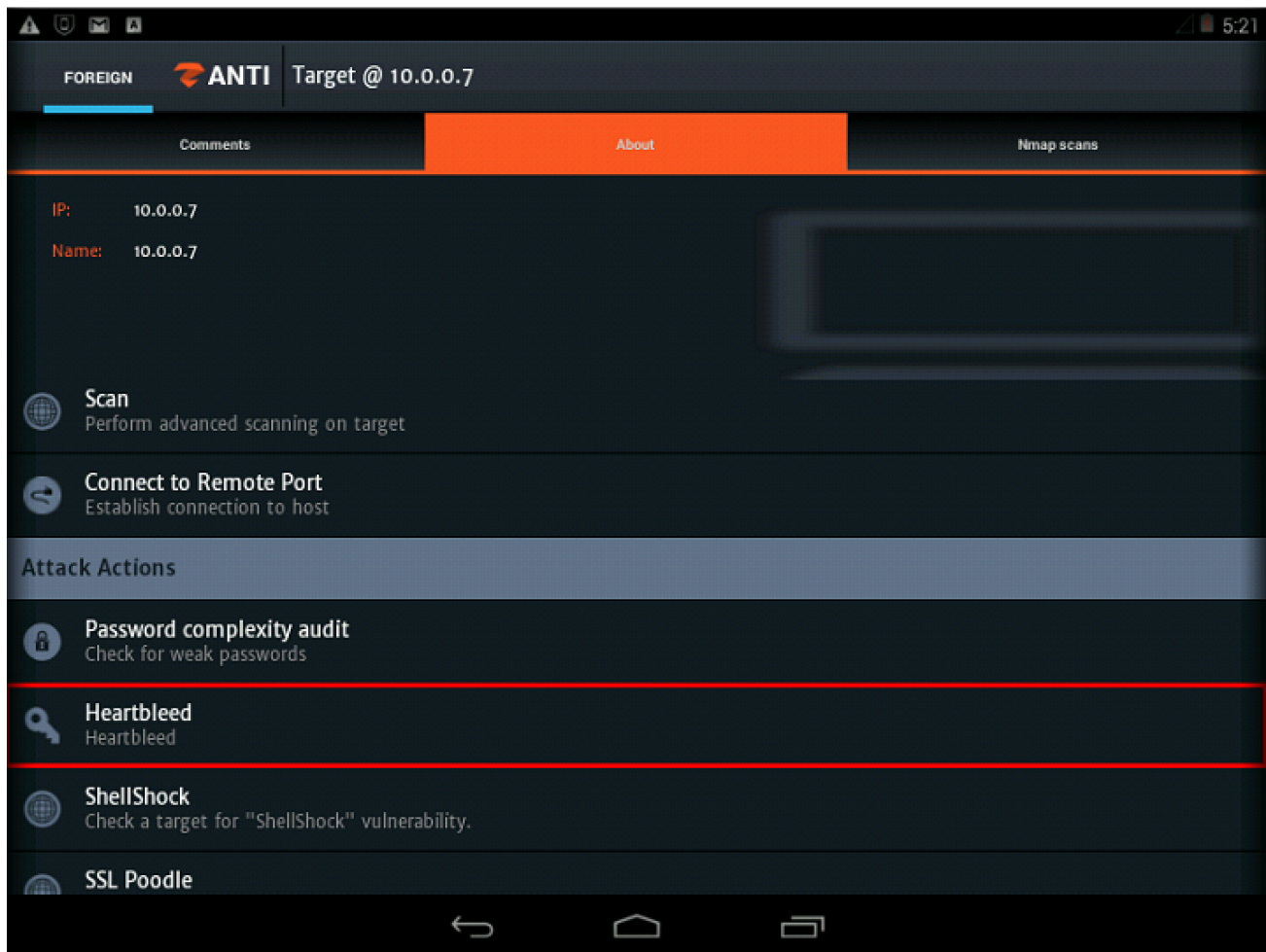


FIGURE 4.30: Attack Options-Heartbleed

38. zANTI scans the target at the provided IP address, the results of which are shown in the screenshot.

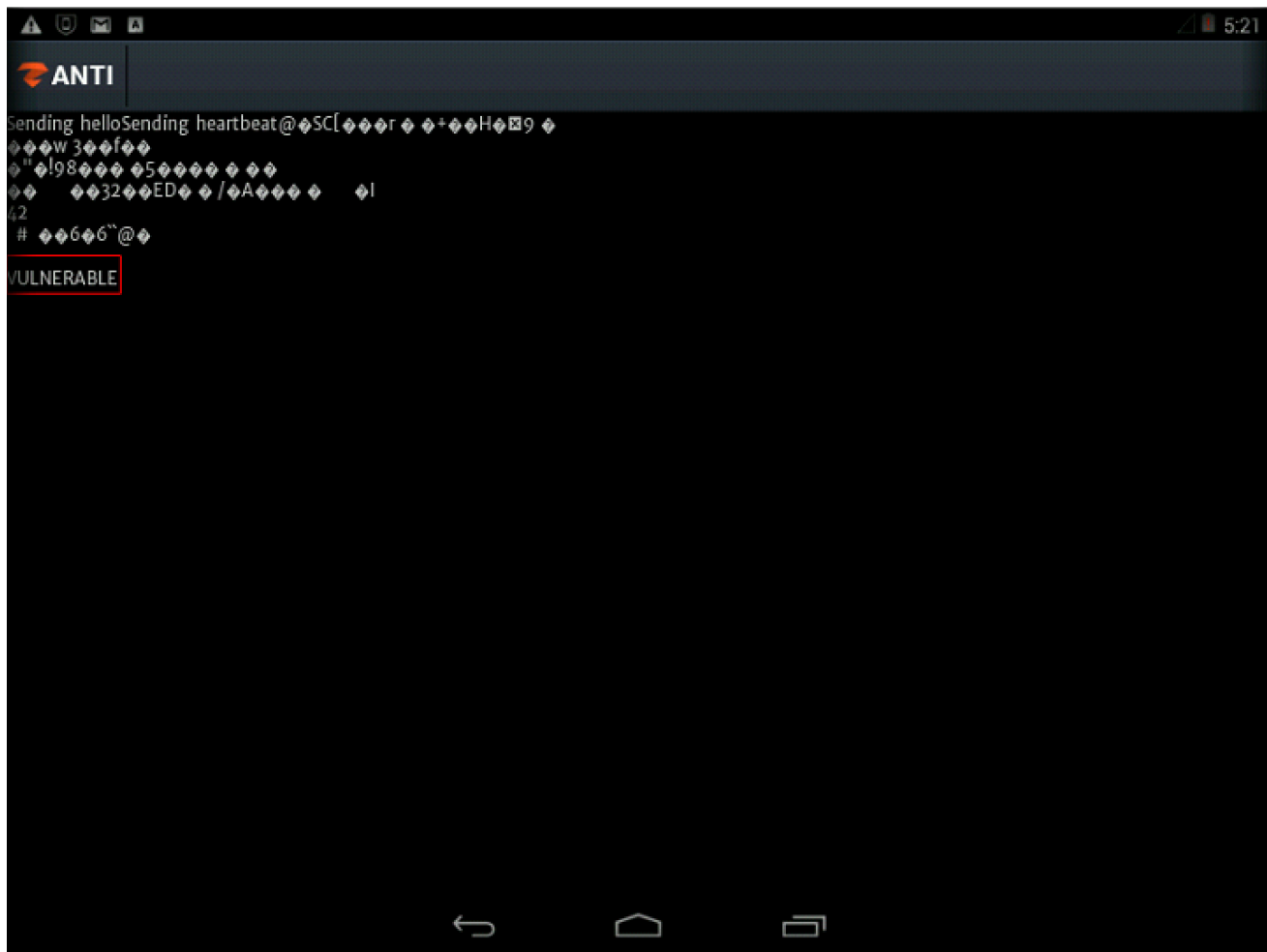


FIGURE 4.31: zANTI shows the Vulnerability Scan Result

39. Similarly, you can perform other vulnerability scans using the **Attack options**.

Lab Analysis

Analyze and document the results related to this lab exercise. Provide your opinion of your target's security posture and exposure through public and free information.