|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name: Nishchal Sreevathsa |  |  |  |  |

Breaking WEP and WPA and Decrypting

the Traffic

Ethical Hacking& Lab 12

Table of Contents

1. [Executive Summary 2](#_Toc409378035)

[Highlights](#_Toc409378036)

[Objectives](#_Toc409378037)

1. [Lab Description Details 2](#_Toc409378038)

[Include Steps Taken, Notes, & Screen Shots demonstrating completion of lab objectives](#_Toc409378039)

1. [Supporting Evidence 17](#_Toc409378040)
2. [Conclusion & Wrap-Up 19](#_Toc409378041)

[Summary with observations, Success & Failures, Challenges](#_Toc409378042)

# Executive Summary

## Highlights

|  |  |
| --- | --- |
|  | In this lab, you will learn how to use various Kali Linux tools to exploit vulnerabilities in the Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) wireless security protocols. The lab cracks the WEP and WPA keys, puts the wireless interface in monitor mode, and decrypts the wireless traffic that has been collected using commands like iwconfig, airmon-ng, aircrack-ng, and airdecap-ng. Both the encrypted and decrypted packet captures are analyzed using Wireshark. |

## Objectives

|  |  |
| --- | --- |
|  | The goal of the lab is to teach you how to use various Kali Linux tools to exploit vulnerabilities in the WEP and WPA wireless security protocols. Decryption of wireless network traffic using WPA and WEP is the result. |

# Lab Description Details

## Include Steps Taken, Notes, & Screen Shots demonstrating completion of lab objectives

**Step 1:** Launch the internal Kali 2 Attack machine with the **Internal IP Address 192.168.1.101**. Once the machine is booted enter the Username as **root** and Password as **toor** and login to the machine and then open the **Linux Terminal**.

**Step 2:** Use the command iwconfig to view the interfaces on your system that are capable of wireless networking. You can use the airmon-ng command to enter monitor mode on a wireless card. Examine the airmonng command's options. The WPA passphrase and WEP key can be cracked using the aircrack-ng command. examine the aircrack-ng command's options.

A screenshot of a computer

Description automatically generated

**Step 3:** The airdecap-ng command is used to decrypt WEP and WPA traffic after the key has been obtained. Examine the airdecap-ng command's settings.

A screenshot of a computer

Description automatically generated

**Step 4:** List the contents of the folders and files in your current working directory. Navigate to the directory named Captures. list the contents of the folders and files in your current working directory.Wepcaptures from wireshark.

**Challenge #1:** With the help of cat command was able to capture the **flag2.txt:** **555616**.

A screenshot of a computer screen

Description automatically generated

**Step 5:** Use Wireshark to decrypt the encrypted capture file. IP addresses and application layer protocol traffic, such as FTP, TELNET, HTTP, SMTP, or POP3, are not visible when the traffic is encrypted.

A screenshot of a computer

Description automatically generated

**Step 6:** Take the file containing a lot of initialization vectors (IVs) and extract the WEP key from it. Type 1 refers to the target's index number. On the screen will appear the WEP Key.

A screenshot of a computer

Description automatically generated

**Step 7:** Unlock the capture file's WEP traffic encryption. The decrypted communication will now be in a freshly produced cap file. enumerate every file and folder in the working directory you are currently in.

A screenshot of a computer

Description automatically generated

**Step 8:** Use Wireshark to access the decrypted capture file. To see the IP Address, put ip in the Wireshark filter pane and click apply.

A screenshot of a computer

Description automatically generated

**Step 9:** View the password PACERS123 for the user by using FTP to filter now. FTP uses unformatted text.

A screenshot of a computer

Description automatically generated

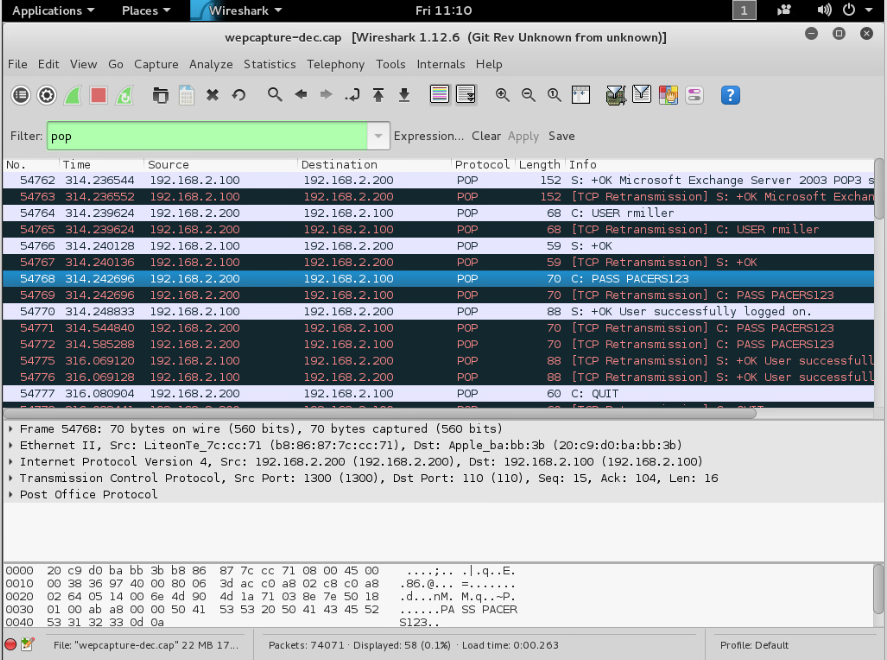
**Step 10:** To view the DNS Traffic, use a filter that includesdns and frame contains "flag".

**Challenge #2:** Captured the **flag3: 88912** in DNS Traffic.

A screenshot of a computer

Description automatically generated

**Step 11:** To inspect the email traffic, type pop in the Wireshark Filter pane. POP is in plain text; see PACERS123's user password.



**Step 12:** In the first POP result frame, right-click and choose Follow TCP Stream. Examine the traffic in plain text. Then select the option to "Filter Out This Stream."

A screenshot of a computer

Description automatically generated

**Step 13:** On the first results frame, use the right-click menu to choose Follow TCP Stream. Examine the traffic in plain text. To view the email on the Cleveland Cavaliers, scroll down.

A screenshot of a computer

Description automatically generated

**Step 14:** To view the telnet traffic, type TELNET in the Wireshark Filter pane. In the initial telnet result frame, right-click and choose Follow TCP Stream. Examine the traffic in plain text. Then select the option to "Filter Out This Stream."

A screenshot of a computer

Description automatically generated

**Challenge #3:** Choose Follow TCP Stream by doing a right-click on the following results frame. Got hold of the **flag4: 876554**.

A screenshot of a computer

Description automatically generated

**Step 15**: To inspect the QOTD traffic, type QOTD in the Wireshark Filter pane. Plain text is used in QOTD content.

**Challenge #4:** Captured the **flag5:818334** after using a QOTD traffic filter.

A screenshot of a computer

Description automatically generated

**Challenge #5:** In the first result frame, right-click and choose Follow TCP Stream. Select the option "Filter Out This Stream." **Flag6:555344** captured

A screenshot of a computer

Description automatically generated

**Step 16:** After selecting File, go to Export Objects and select HTTP. Choose "Save All."

A screenshot of a computer

Description automatically generated

**Step 17:** On the desktop, save the folder name as wep.

A screenshot of a computer

Description automatically generated

**Step 18:** View the Cleveland Cavaliers' pictures by opening the WEP folder.

A screenshot of a computer

Description automatically generated

**Step 19:** List the contents of the folders and files in your current working directory. encrypt the capture file and open. IP addresses and application layer protocol traffic, such as FTP, TELNET, HTTP, SMTP, or POP3, are invisible when the traffic is encrypted. Use an IP filter to see if any results appear.

A screenshot of a computer

Description automatically generated

**Step 20:** Use a dictionary attack to extract the WPA password or key from the capture file. For the intended network index number, use type 2. Boneless's WPA Passphrase will be shown.

A screenshot of a computer

Description automatically generated

**Step 21:** Open the capture file and decrypt the WPA traffic. The decrypted communication will now be in a freshly produced cap file. enumerate every file and folder in the working directory you are currently in.

A screenshot of a computer

Description automatically generated

**Step 22:** Use Wireshark to access the decrypted capture file. Packets were shown when filtered by IP address.

A screenshot of a computer

Description automatically generated

**Step 23:** FTP traffic can be seen in the wireshark filter pane when it is filtered with ftp. You will be able to examine P@ssw0rd's password because FTP is in plain text.

A screenshot of a computer

Description automatically generated

**Step 24:** Email traffic can be observed in the Wireshark filter pane when filtered with pop. You will be able to examine P@ssw0rd's password because POP is in plain text.

A screenshot of a computer

Description automatically generated

**Step 25:** Once you perform a right-click on the initial POP result frame, choose Follow TCP Stream. Examine the correspondence regarding the Spurs in San Antonio.

A screenshot of a computer

Description automatically generated

**Step 26:** Click File, then select HTTP and click Save all after swiping down to Export Objects.

A screenshot of a computer

Description automatically generated

**Step 27:** Save the folder to the desktop with the name "wpa."

A screenshot of a computer

Description automatically generated

**Step 28:** Explore the WPA folder to see San Antonio Spurs images.

A screenshot of a computer

Description automatically generated

# Supporting Evidence

**Screenshots, Research, Etc.**

**A screenshot of a chat

Description automatically generated**

**A screenshot of a computer

Description automatically generated**

**A screenshot of a computer

Description automatically generated**

**A screenshot of a computer

Description automatically generated**

# Conclusion & Wrap-Up

## Summary with observations, Success & Failures, Challenges

Throughout this lab, you successfully decrypted wireless WEP and WPA network traffic using the iwconfig, airmon-ng, aircrack-ng, and airdecap-ng commands. After the communication was decrypted, you examined the plaintext data within it in Wireshark to confirm the findings.

**Observations:**

* The WEP key and WPA passphrase from the supplied capture files could be cracked by Aircrack-ng.
* Using the cracked keys, Airdecap-ng was able to decrypt the WPA and WEP communications successfully.
* Visibility into encrypted versus decrypted traffic was made possible by Wireshark.

**Success:**

* Both WPA and WEP encrypted wireless communication has been decrypted.
* Taken credentials and other data in plaintext out of the packet that had been encrypted.

**Risks:**

* Sensitive employee or customer information that could cause data breaches if accessible by attackers may be found in wireless communication that has been cracked.
* Wireless security protocols such as WEP and WPA have vulnerabilities that might make it simple for attackers to get access to internal business networks.
* Using credentials that have been compromised, attackers can access the users' other systems and services.
* Inadequate wireless encryption offers minimal defense against interceptions and man-in-the-middle attacks.
* Modern hardware and operating systems may not support outdated wireless protocols, or they may outright forbid them.
* Legal issues arise if hacking or illegal access are not stopped or discovered in a timely way.

**Remediations:**

* To find and fix vulnerabilities, conduct routine wireless penetration tests.
* To improve wireless access security, put in place an 802.1X authentication mechanism such as RADIUS.
* Utilize VLANs to divide wireless networks into distinct SSIDs in order to restrict access.
* Use wireless intrusion prevention systems to identify malicious APs and attacks.
* Use enterprise mode with lengthy, complicated passphrases or strong encryption such as WPA2/WPA3 PSK.
* Update wireless AP firmware and settings frequently to take advantage of the newest security features.
* Inform users on the best practices for encryption and authentication in wireless security.
* Logs of wireless access should be kept and reviewed in order to spot any unauthorized connections.
* If it's not absolutely necessary, remove support for antiquated and unsafe wifi protocols like WEP.