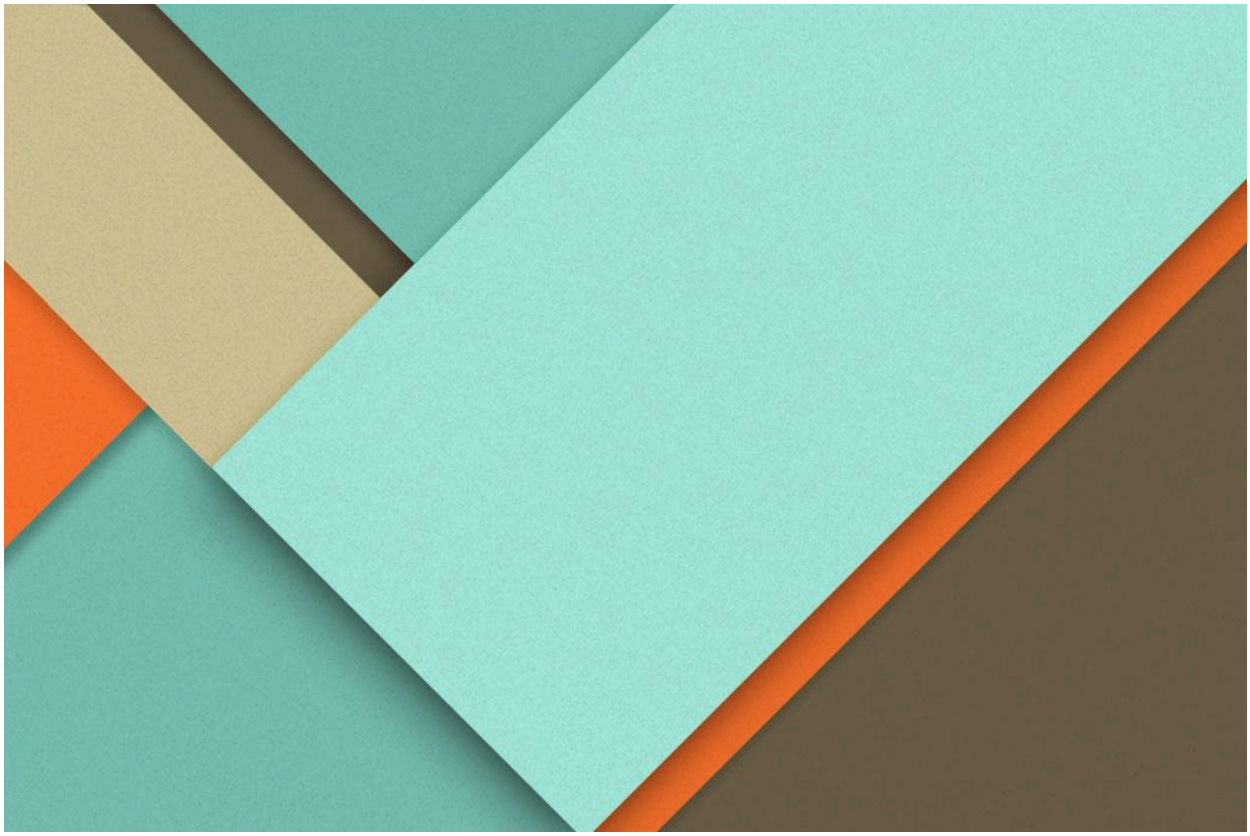


DEPI Project

24.10.2024

—

Name	Email
Nada Essa	nadaessa086@gmail.com
Nehal Sherif	nehalsherif54@gmail.com
Raghad Atef	raghad.atef20@gmail.com
Asmaa Abderahman	asmaaabdelrhman7654@gmail.com
Heba Samir	heba.samir@ejust.edu.eg

Overview

How can we effectively hide a malicious payload within an image, deliver it to unsuspecting users via a phishing email, and subsequently detect and prevent similar attacks using network security tools?

Tasks

Steghide to extract data from an image

1. Introduction

The objective of **Steghide** is to securely embed and conceal data (such as text, files, or messages) within image or audio files in a way that is imperceptible to the human eye or ear. This allows for covert communication or data storage, while protecting the hidden content from detection and unauthorized access.

2. Practical example

First I uploaded an image and created a text file, then used the above command to hide the text file inside the image and the image didn't change to the user though the text file is hidden inside of it.

After that, I used the above command to extract the data inside the image and successfully got the text file extracted from the image.

Phishing Simulation Task Report using GoPhish

1. Introduction

This report documents the process of conducting a phishing simulation using GoPhish, a widely used open-source phishing framework. The objective of the task was to create and launch a phishing email campaign targeting users with a fake job offer from Google. The email included an embedded image with a malicious link, designed to test the vulnerability of recipients to phishing attacks.

2. Objective

The main goal of this task was to simulate a realistic phishing attack, designed to:

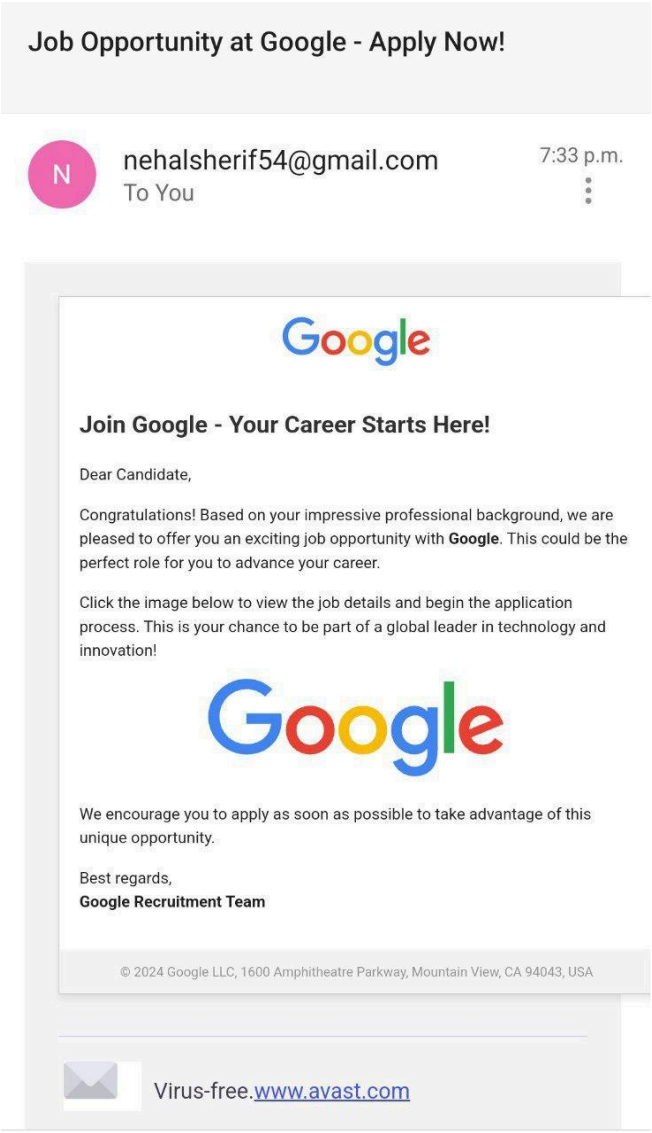
- Trick recipients into clicking on a malicious link by offering a job opportunity at a reputable company (Google).
- Embed the malicious link within an image to bypass suspicion and track user interaction with the email.

The task was carried out as part of a broader cybersecurity awareness campaign aimed at educating users on the dangers of phishing emails.

3. Phishing Email Content

The phishing email was designed to resemble a genuine job offer from Google. The key components of the email included:

- A **subject line** to catch the recipient's attention: "Job Opportunity at Google - Apply Now!"
- **Body text** that described a fake job offer and encouraged the recipient to click an embedded image to get more information.



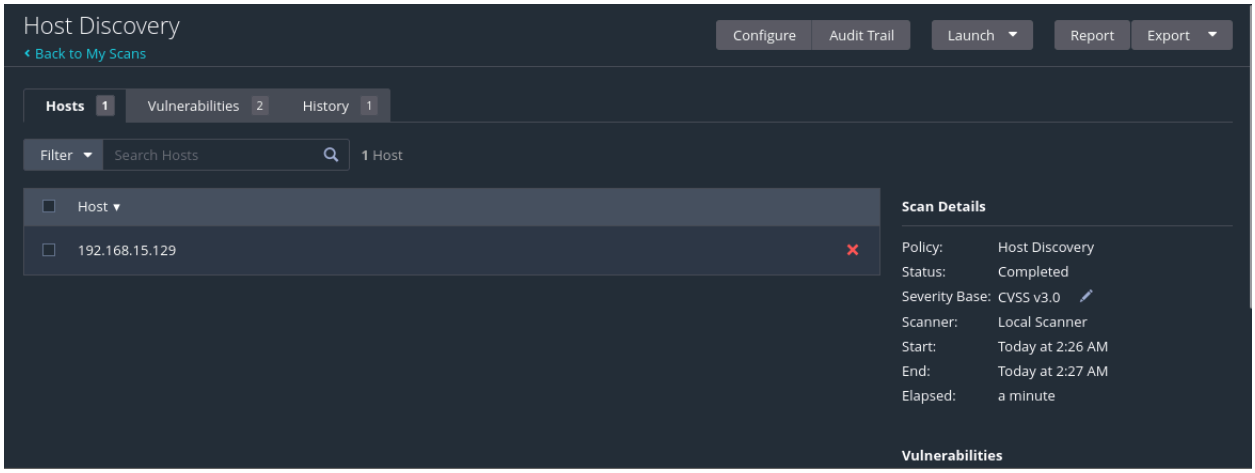
Conclude a malicious activity and Scan the device network

Setup

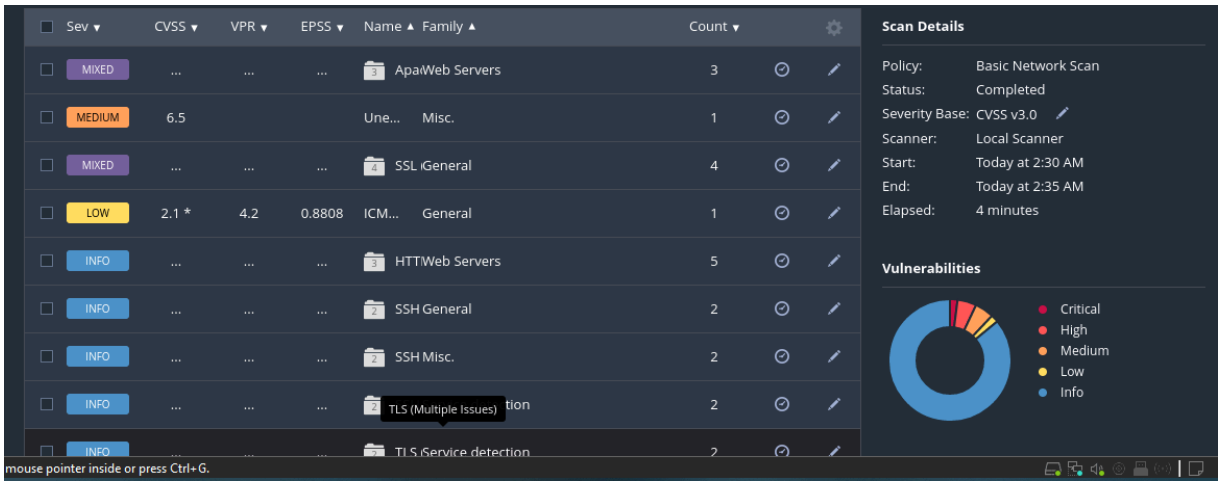
- Target Machine (Victim): Ubuntu Desktop With SSH, Telnet and Apache2 enabled (IP: 192.168.15.129)
- Attacker Machine: Kali Linux with Nessus installed.
- Network Range: 192.168.15.0/24 (Local Network)

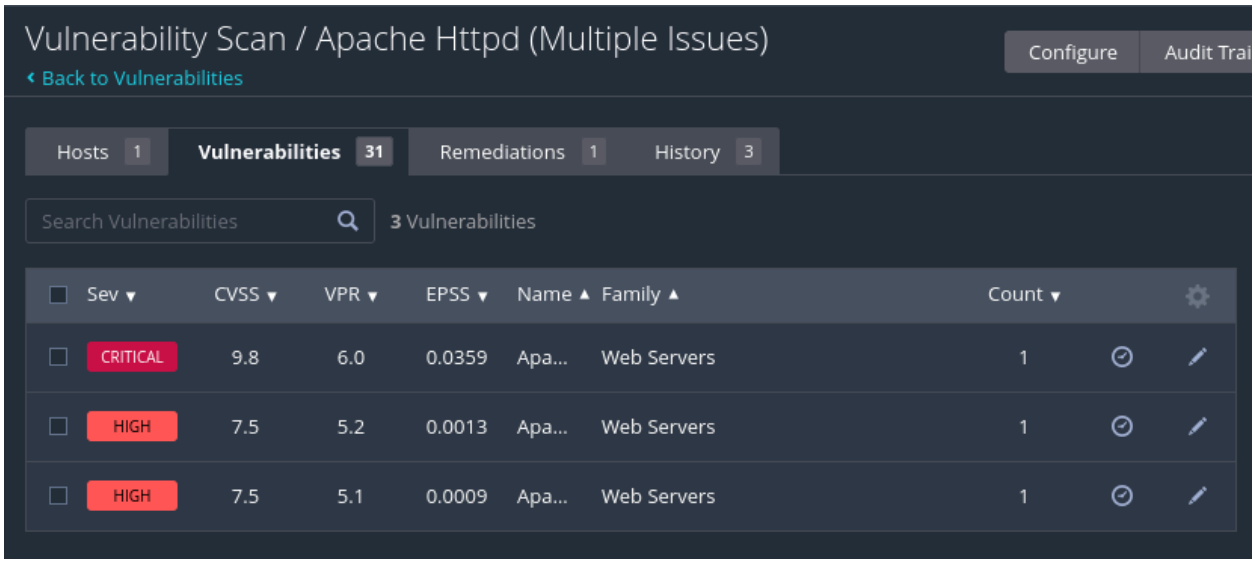
Scenario

- Scanning the network using Nessus to find the current Hosts.



- Applying Network Scanning on the victim's machine.





- Applying Web Application Scanning on the victim's machine.