Packet Quest Overview and User Manual

Anwuli Ajabor
anwulicreates@gmail.com

***Abstract*—This offers a comprehensive guide to Packet Quest, including an overview of the game, detailed instructions on how to use its features, and step-by-step instructions for installing it on your personal computer.**

I. Introduction

Packet Quest is a pygame based project that uses Scapy (Python) to handle real-time packet generation in order to provide a gamified learning tool for studying ARP (Address Resolution Protocol). Discover how ARP functions in an entertaining and interesting way. It also includes a segment for packet generation with protocols like arp and icmp. Learn about some computer networks easier.

II. Motivation

My experience working as a staff member at a Florida Institute of Technology (FIT) Cyber Summer Camp served as an inspiration for gamifying this project. The idea to transform that energy and curiosity into an organized learning tool emerged from seeing children play "Packet Wars" with enthusiasm during the camp. By fusing education and fun, this project hopes to make networking and cybersecurity topics understandable to students of all ages.

III. Proposed Approach

The goal of Packet Quest is to develop an interactive and instructive game that engrosses players in a captivating mystery story while teaching network protocols and cybersecurity topics. Using networking technologies and procedures, players take on the role of a detective entrusted with solving a murder mystery. Finding and following IP addresses to their matching MAC addresses, spotting ARP spoofing attempts, and resolving technical issues that are woven into the narrative are all part of the game-play. Through interactive game play components and minigames, the game will concentrate on teaching fundamental networking principles, such as ARP, ICMP, and packet analysis. Through gamification, game design prioritizes player interaction and transforms technical education into an engaging detective game.

IV. Networking Concepts in Gameplay

A. ARP(Address Resolution Protocol)

ARP is a network protocol used to map an IP address to its corresponding MAC (Media Access Control) address. In a local network, devices use ARP to determine the MAC address of the device they want to communicate with, allowing data packets to be correctly routed at the data link layer

B. IP (Internet Protocol)

The Internet Protocol is a fundamental protocol in the network layer that enables the addressing and routing of data across diverse networks.

C. ICMP (Internet Control Message Protocol)

Internet Control Message Protocol is used to report errors and perform network diagnostics. In the error reporting process, ICMP sends messages from the receiver to the sender when data does not come though as it should.

D. IP packet generation with ICMP Protocol

IP is a layer 3 protocol on its own; to create a full packet structure, it needs an encapsulated protocol (such as ICMP, TCP, or UDP). Malformation results from the packet's incompleteness in the absence of a transport or network-layer protocol payload. In order to prevent malformed packets, ICMP completes the IP packet structure, provides a legitimate payload, and complies with protocol specifications.

E. ARP Spoofing

ARP spoofing is a type of attack where a malicious actor sends falsified ARP messages to associate their MAC address with the IP address of a legitimate device, allowing them to intercept or disrupt traffic. A hacker commits an ARP spoofing attack by tricking one device into sending messages to the hacker instead of the intended recipient. For example, hacker mapping their IP address to same mac as a legitimate device like a router and could be mistaken as same device.

F. Anti-ARP Spoofing Techniques

Preventing ARP Spoofing: Key Strategies

- Static ARP Entries
  - Manually set IP-to-MAC address mappings on network devices.
  - Restrict usage to known and authentic mappings to prevent ARP table poisoning.
- Detection Tools
  - Use tools like Wireshark, Arpwatch, and XArp to monitor ARP traffic.
  - Identify unusual ARP behavior, such as duplicate IP-to-MAC address mappings, and alert administrators to spoofing attempts.
- Real-Time Attack Detection
  - Scan ARP traffic for irregularities to detect spoofing attacks as they occur.
- Encryption Techniques

- Implement encryption methods like IPsec or VPNs to secure network communications.
- Prevent attackers from decrypting or altering encrypted communication, even if ARP packets are spoofed.

V. How To Install Packet Quest

Firstly, Download files from github repo, ensure your environment has all base requirements in requirements.txt.

Install Python 3.9 or higher from python.org.

Install required libraries using:

```
pip install pygame moviepy scapy
```

Run the game by executing:

```
python PacketQuest_scratch.py
```

VI. How to Download Files from the GitHub Repository for Packet Quest

Welcome to this tutorial! This guide will help you retrieve files from the GitHub repository for Packet Quest.

Step 1: Visit the Repository Open a web browser. Go to: https://github.com/Anwuli/Packet-Quest.

Step 2: Explore the Repository On the main page of the repository, you'll see a list of folders and files. This is where all the game files are stored.

To Download the Entire Repository On the main repository page, locate the green "Code" button near the top right.

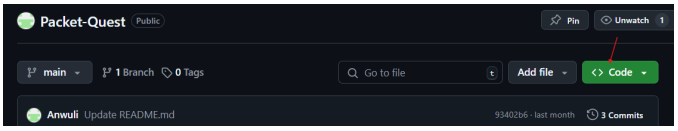

Fig. 1. Code Button

Click on the "Code" button and select "Download ZIP" from the dropdown menu. The repository will be downloaded as a .zip file. Extract the file on your computer to access all the game files.

If you're familiar with Git, you can clone the repository using the following command in your terminal:

git clone https://github.com/Anwuli/Packet-Quest.git

This will create a local copy of the repository on your machine.

VII. How To Play Packet Quest from Terminal

Open location where Packet quest is saved in a terminal. For instance, on windows: using cd documents/packet-quest

run python PacketQuest.py

The game window will then open up.

Left-click to interact with buttons and select options.

Upon launching the game, the main menu offers:

- Start: Begin your investigation at the Hartley Mansion.
- Select Level: Jump to specific parts of the game.
- Bonus: Learn ARP basics and networking concepts.
- Credits: View game creators and contributors.
- Quit: Exit the game.

Fig. 2. Game Main Window

VIII. GamePlay Overview

Click start to start the game. A new window with a short film as seen in Fig 3 describing the mystery will pop up, pay attention to clues as it will be useful in long run.

Fig. 3. Short Film

Investigate the crime scene in Hartley Mansion.

Use clues like IP addresses to identify devices and gather evidence.

Key Actions:

Solve riddles to progress through the storyline.

Enter IP addresses in text fields as seen in Fig. 4.

Incorrect entry of correct IP format will result in receiving an error message as seen in Fig 5. Retry with correct format and click enter on keyboard.

IX. Inmate Contact Portal Overview

The Inmate contact portal is a feature in Packet Quest designed to help players engage with in-game characters using network protocols.

Here's how to use the portal: **Accessing the Portal**: Click levels button in main window then select Inmate Contact

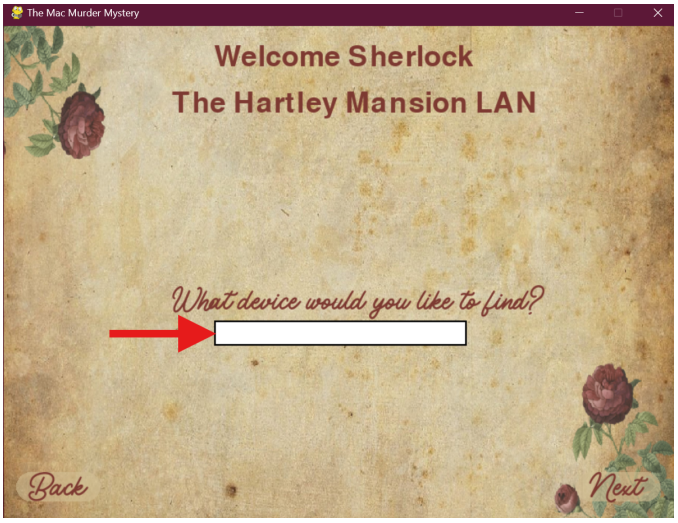

Fig. 4. Enter IP Clue

Fig. 5. Incorrect IP Entered

Portal. This is a key part of the investigation where you'll contact a suspected character.

You will need to input the following details: - *Packet Count*: Enter the number of packets you want to send to the target device. - *Payload*: Input a message (payload) that will be included in the packet. - *Destination IP*: Provide the IP address of the device you want to contact.

Protocol Selection: Choose the network protocol to use for communication, ARP or ICMP.

Send and Receive: Once the information is entered, click *Generate* to send the packets.

If any input is incorrect, an error message will appear, guiding you to correct the details before proceeding. Be sure to check for valid IP addresses and appropriate packet counts.

By using the Inmate Contact Portal, players will test their knowledge of network protocols while progressing through the mystery, uncovering clues, and advancing the storyline.

X. ARP Spoofing Demo

This provides instructions for using the ARP spoofing script written in Python with the Scapy library. The script allows you to send ARP responses to a target device, associating the spoofed IP with your system's MAC address. This technique is often used in penetration testing and network analysis. The file, ArpSpoofingSimulator.py can be ran in terminal to simulate an Arp spoofing attack that can be seen in wireshark. An error indicated in your Wireshark capture, a duplicate use of certain ip address for different MAC addresses indicates a successful spoof. The ARP table of systems may not change due to the restrictions of operating system.

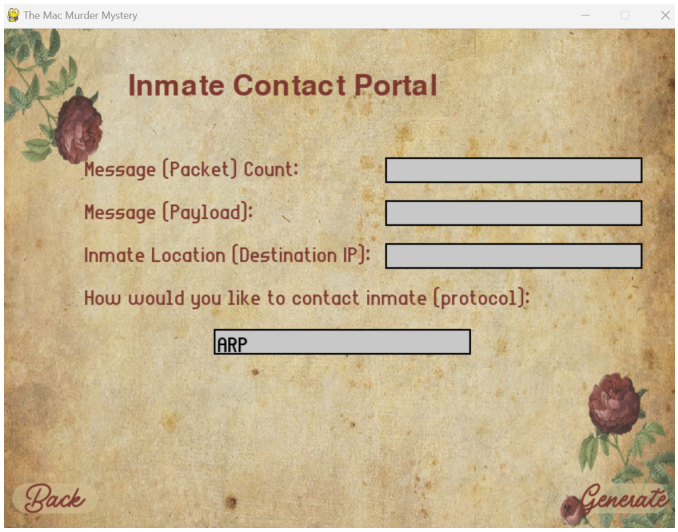

Fig. 6. Packet Generator

To begin analysis, Download Wireshark and start a capture of your active network.i.e if connected to WiFi, capture WiFi. Then run the code in terminal, in directory where file is saved.

```
python ArpSpoofSimulator.py
```

You will be prompted to enter the following information:

- Your laptop's IP address: Enter the IP address of your computer.
- target laptop's IP address: Enter the IP address of the target computer.
- Router/gateway IP address: Enter the router's or gateway's IP address.
- Your MAC address: Enter your system's MAC address.

The script will begin spoofing the ARP cache of the target system and the router/gateway. To stop the process, press `Ctrl + C`.

A. Requirements

Before running the script, ensure you have the following:

- Python 3.9 or higher installed on your system.
- The Scapy library installed. Install it using:

```
pip install scapy
```

- Administrator (root) privileges for network access.

B. Script Overview

The script is designed to send ARP spoofing packets to a target system. The target will receive an ARP response indicating that your machine is the specified IP address.

The ARP spoofing process involves the following steps:

1) The script accepts user inputs for the following values:
   - Your computer's IP address.
   - target computer's IP address.
   - Router/gateway IP address.
   - Your computer's MAC address.

2) The script sends ARP responses to the target device, associating the spoofed IP address with your system's MAC address.
3) This process repeats every 2 seconds until interrupted.

C. Disclaimer

This script should only be used for educational purposes or on networks you own or have explicit permission to test. Unauthorized ARP spoofing can disrupt network operations and is illegal in many regions.

XI. Key Features

- Learn and apply ARP concepts in engaging scenarios.
- Generate and analyze ARP and ICMP packets using in-game tools.
- Access bonus materials and a glossary for networking terms.

XII. Future Enhancements for Packet Quest

- Fully adapt the game using a more robust engine like Unity.
- Include support for additional network protocols.
- Introduce new storylines or expand on the initial plot.
- Develop adaptations based on popular Sherlock Holmes stories.
- Create engaging mini-game levels for additional gameplay variety.
- Explore multiple endings in a gamebook-style narrative.

XIII. Conclusion

With the help of gaming and technical education, Packet Quest hopes to become a distinctive educational resource in the future. Collaborative multiplayer options, downloadable materials, and expansions are all envisioned for increased instructional and entertainment value. Packet Quest will help users deepen their knowledge of the ARP protocol, easy packet generation, and spoofing, as well as how to mitigate spoofing.