

FLORIDA INTERNATIONAL UNIVERSITY



VIP/Senior Project Final Presentation Fall 2024

K-9 Packet Sniffer

Team Members: Edward Medina, Sharek Rendon, Maritza Medina, Tiago Muller, Carlos Imery

Professor: Masoud Sadjadi

FLORIDA INTERNATIONAL UNIVERSITY





Problem Definition

Network administrators and security professionals often rely on tools like Wireshark to capture and analyze network traffic. However, the absence of user-based session management in these tools is a critical issue, as it leads to challenges such as:

- **Manual File Management:** Users must manually save, organize, and track capture files.
- **No Built-in user authentication:** Securely associating sessions with specific individuals is challenging, highlighting the need for robust user access control.
- **Risk of Data Loss or Mismanagement:** Without proper organization, session data is at risk of being misplaced or mishandled, posing a security



Project Management/Use Case

A robust, user-friendly tool for monitoring and analyzing network traffic. This tool is designed to help IT professionals, network engineers, cybersecurity specialists, and even everyday users efficiently monitor and secure their networks by capturing and analyzing packet data.

Existing Tools:

- Tools like Wireshark are widely used for network traffic analysis
- They allow users to capture and analyze network packets in real-time

Manual Session Management: Users can only download or save capture files themselves, leading to potential disorganization or data loss.

No User-Based Access Control: Anyone with access to the system can view or manipulate saved session files.

Scalability Issues: Managing numerous capture files becomes cumbersome, especially in multi-user environments.

Steep Learning Curve: The interface can be overwhelming for beginners, and certain features lack user-friendly implementation.



K9

Individual User Stories

Role & Contributions



User Stories: Edward Medina

Role:

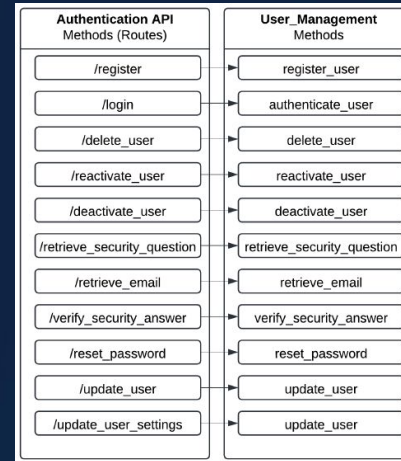
- Product Owner/Team Lead
- Full Stack Developer

Main Focus:

- User Authentication Implementation
- Database Configuration
- Saved Sessions Functionality

Key Contributions:

- Designed and implemented a secure user authentication system with sign-up, sign-in, and logout functionality.
- Configured the K-9 Data database for optimal performance and reliability.
- Debugged and optimized front-end and back-end components, enhancing overall functionality across the project.
- Saved Sessions, Authentication API, UserManagement, polishing Sniffer API





User Stories: Sharek Rendon

Role:

- Full Stack Developer

Main Focus:

- Backend Integration
- Packet Filtering
- Interactive Dashboard Display
- Database Connectivity

Key Contributions:

- Mapped back-end functions, such as the Python packet sniffer file, to the dashboard's capture features for smooth integration between data processing and the user interface.
- Developed a filtering function in Java, using a packet filtering template, enabling users to analyze specified packet types in real-time.
- Added a feature in the packet sniffer script to scan available interfaces on the device and an interactive display for packet details
- Connected the database server to capture and store packets generated by the K-9 software.
- Contributed to the development of packet details, traffic summary, and real-time packet display

```
// Save capture to backend
const handleSaveCapture = () => {
  fetch('http://127.0.0.1:5000/save', {
    method: 'POST',
    headers: { 'Content-Type': 'application/json' },
    body: JSON.stringify({
      username: usercredentials.username, // Send the username with the request
      packets: capturedPackets // Optionally send the captured packets, or modify the backend to handle it
    })
  })
  .then(response => response.json())
  .then(data => {
    alert(data.message);
  })
  .catch(error => console.error('Error:', error));
};
```

```
# Endpoint to get network interfaces
@app.route('/interfaces', methods=['GET'])
def get_interfaces():
    interfaces = psutil.net_if_addrs()
    interface_names = list(interfaces.keys())
    return jsonify({"interfaces": interface_names}), 200
```

```
// Start packet capture
const handleStartCapture = () => {
  if (!selectedInterface) {
    alert("Please select an interface first.");
    return;
  }

  fetch('http://127.0.0.1:5000/start', {
    method: 'POST',
    headers: { 'Content-Type': 'application/json' },
    body: JSON.stringify({ interface: selectedInterface }) // Pass the selected interface to the backend
  })
  .then(response => response.json())
  .then(data => {
    console.log(data.message);
    setIsCapturing(true);
    setIsPaused(false);
  })
  .catch(error => console.error('Error:', error));
};

// Stop packet capture
const handleStopCapture = () => {
  fetch('http://127.0.0.1:5000/stop', { method: 'POST' })
  .then(response => response.json())
  .then(data => {
    console.log(data.message);

    if (Array.isArray(data.packets)) {
      const newPackets = data.packets;
      setCapturedPackets(prevPackets => {
        const updatedPackets = [...prevPackets, ...newPackets];
        updateTrafficSummary(updatedPackets);
        return updatedPackets;
      });
    } else {
      console.error("Packets data is not an array:", data.packets);
    }
  })
};
```



User Stories: Maritza Medina

Role:

- Front End Developer

Main Focus:

- Prototype creation
- JavaScript/CSS page creation
- Ensuring intuitive functionality/appearance

Key Contributions:

- Designed the rough draft of our project using Axure RP.
- Incorporated React into our project to bring it to life, creating the project's buttons, links, pages (sign in/sign up, forgot password, dashboard, session management/capture control, and profile settings), and more via JavaScript.
- Styled the pages/buttons/links to represent the FIU color scheme.
- Established an overall attractive and intuitive appearance to ensure optimal user experience.

```
return (  
  <div className="container">  
    <div className="title">  
      <h1>Sign In</h1>  
    </div>  
  
    <div className="welcome">  
      <p> Welcome! Please sign-in below to begin sniffing.</p>  
    </div>  
  
    <div className="signup">  
      <p>Don't have an account? <Link to="/sign-up">Sign Up</Link></p>  
    </div>  
  </div>  
)
```

```
/* Styling for the title */  
.title h1 {  
  font-family: Roboto;  
  margin-bottom: 0px;  
  font-size: 3rem;  
  color: #FFFFFF;  
}
```



User Stories: Tiago Muller



Role:

- Pentester / Security Backend Developer

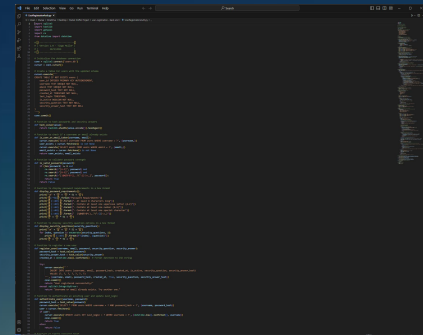
Main Focus:

- Finding Vulnerabilities
- Fixing Vulnerabilities
- Developing backend security solutions
 - Input Sanitization
 - User Authentication
- Create Risk Matrix based on vulnerabilities found such as CWEs (Common Weakness Enumeration)

Key Contributions:

- Ran several vulnerabilities testing tools such as Bandit for Python files, ESLint to find problematic patterns and enforce best practices, OWASP and some more.
- Assisted in developing the user authentication part of the backend development in Python, to validate users upon logging in, making sure the inputs are sanitized to prevent command injection, passwords are hashed, security question for password reset and made sure that data is stored securely.
- Created a risk matrix as seen to the right of this slide, which includes the main CWEs (Common Weakness Enumeration) that were found by the Pentesting programs, all of which were either fixed or attempted to get fixed, those that were not fixed were analyzed for Disaster Recovery and Business Continuity efforts to make sure that we have solutions in place in case those vulnerabilities are exploited.

Risk	Likelihood	Impact	Severity (Priority)
CWE-78: OS Command Injection	High	High	Critical
CWE-94: Code Injection	High	High	Critical
CWE-605: Multiple Port Binds	Medium	Medium	Moderate
Unused Variables (React)	Low	Low	Minor
Unknown Property 'class' (React)	Medium	Medium	Moderate
Unescaped Entities (React)	High	Medium	High
Missing Props Validation (React)	Medium	Medium	Moderate





User Stories: Carlos Imery

Role:

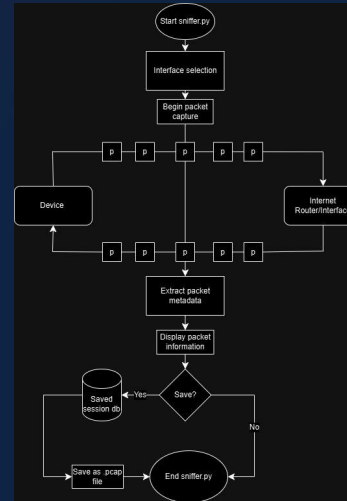
- Backend Developer

Main Focus:

- Designing and creation of sniffer python program (prior to front-end implementation)
 - a. Interface Selection
 - b. Packet extraction
 - c. Protocol Support
 - d. Protocol Breakdown
- Packet Capture Verification and Validation
- Captured Packets Storage to SQL Database

Key Contributions:

- Created our packet sniffing protocol with support for multiple protocols (TCP, UDP, HTTP, DNS, ARP, IP, and IPv6) - sniffer has capturing, displaying, filtering, and saving/exporting capabilities.
- Implemented methods for the individual packets to be saved to a 'captured packets' table within our SQL Database.
- Validated sniffer program by comparing packet capture results with well-known packet capture tools available in the market (i.e, Wireshark).



Available interfaces:

1. Ethernet 2 (18-C0-4D-97-BB-8C)
 2. Local Area Connection (00-FF-F4-BD-5E-BB)
 3. Local Area Connection* 2 (9A-8D-46-DC-D5-D4)
 4. Wi-Fi (98-8D-46-DC-D5-D4)
 5. Bluetooth Network Connection (98-8D-46-DC-D5-D8)
 6. Teredo Tunneling Pseudo-Interface (00-00-00-00-00-00-E0)
- Enter the interface number to sniff on (or leave empty for all):

Captured Packets:

#	Source IP	Dest IP	Src Port	Dest Port	Protocol	Seq Number	Ack Number	F
1	185.203.218.104	10.0.0.65	N/A	N/A	udp	N/A	N/A	N
2	185.203.218.104	10.0.0.65	N/A	N/A	udp	N/A	N/A	N



K9

Software Design Breakdown



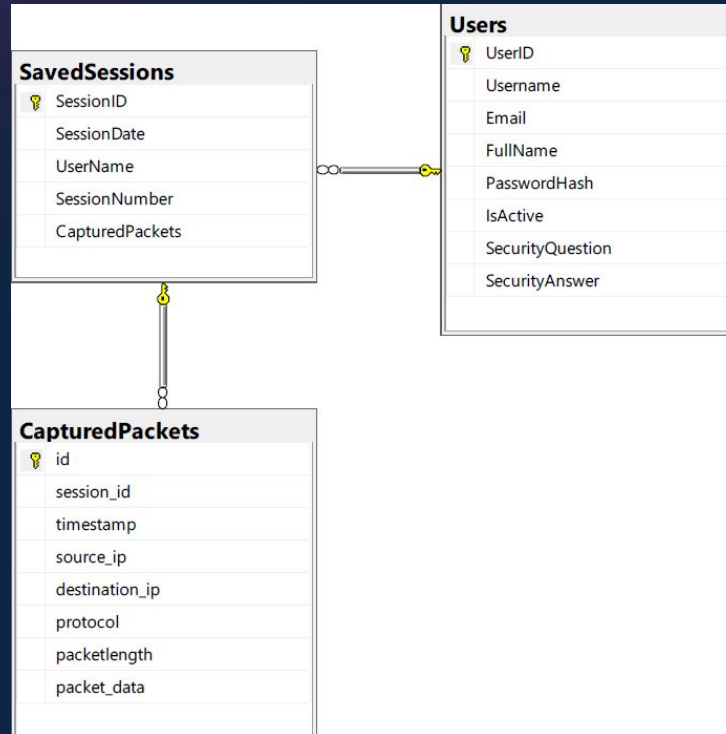


Sequence Diagram - System Design



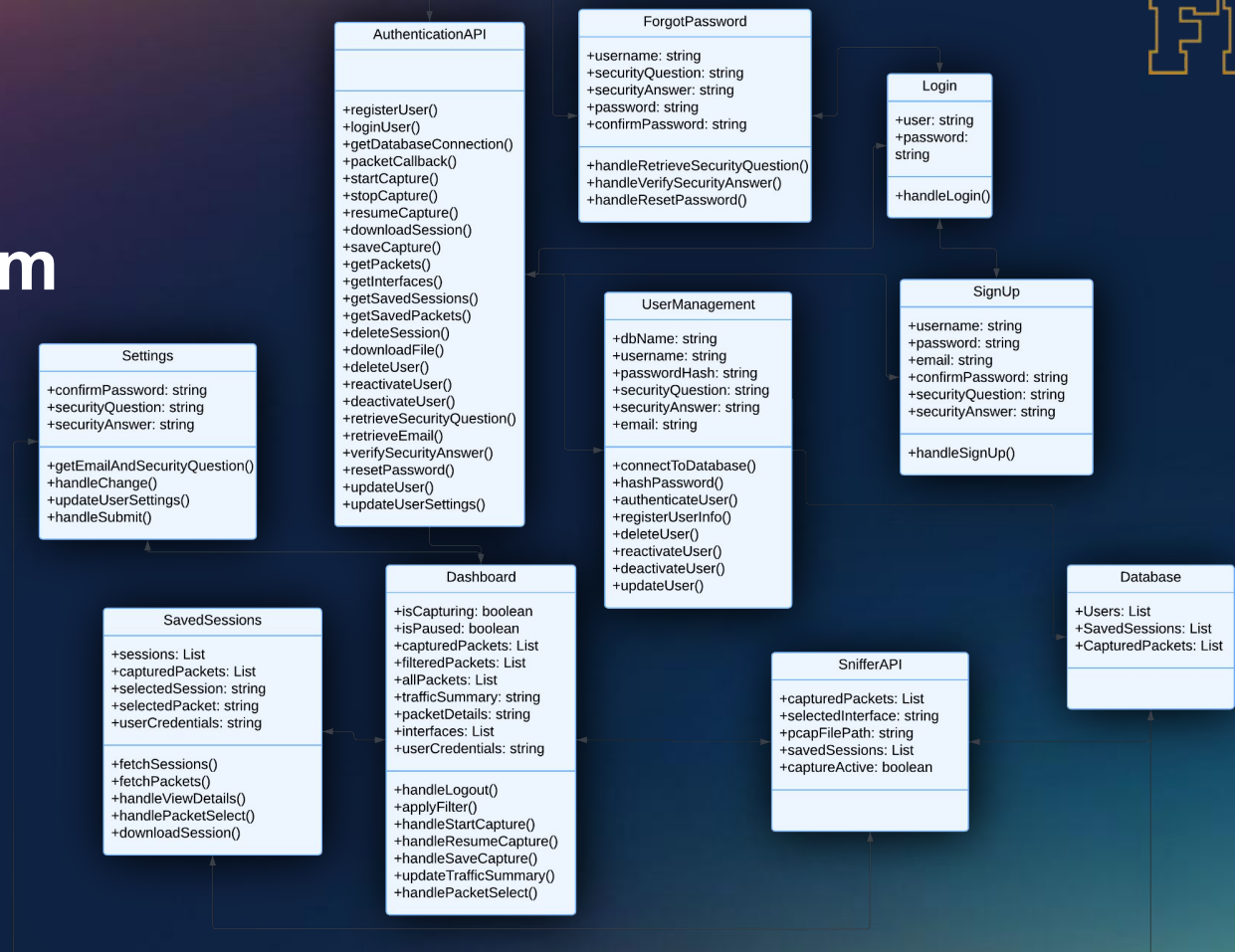


Database Schema Design





Class Diagram





K9

Software Breakdown

User Authentication Pages: Sign In



Sign In

Welcome! Please sign-in below to begin sniffing.

Don't have an account? [Sign Up](#)

Username

Password

☐ Remember me

[Forgot your password?](#)

 [Sign In](#)

User Authentication Pages: Sign Up

Sign Up

We would love to have you join our sniffer community! Sign-up below to begin.



Sign Up

By clicking the "Sign Up" button, you are creating an account, and you agree to the Terms of Use.

[Back to Sign In](#)

User Authentication Pages: Forgot Password

Forgot Password

Username

Retrieve Security Question

[Back to Sign In](#)

Forgot Password

What was the name of your first pet?

Answer

Submit Answer

[Back to Sign In](#)

Forgot Password

Enter new password

Reset password

[Back to Sign In](#)

User Authentication Pages: Settings

Settings

Username:

Email:

Password:

Confirm Password:

Security Question:

What was the name of your first pet? ▾

Security Answer:

Answer to security question

Update Settings

Back to Dashboard

Capture Pages: Dashboard

 Saved Sessions Apply Filter Hello,  Log Out

Your Packets in Real-Time

Start Capture Stop Capture Resume Capture Save Capture

Select Your Interface:

Interface 1 - vEthernet (Default Switch) ▾

Current Interface: vEthernet (Default Switch)

Your Network Traffic Summary

Total Packets: 0
TCP: 0
UDP: 0
ICMP: 0
Other Protocols: 0

Packet Details

Select a packet to view details.

Capture Pages: Saved Sessions

Saved Sessions Hello, 

- Session 1 - 11/30/2024 - 19 packets
[Download](#)
- Session 2 - 11/30/2024 - 25 packets
[Download](#)
- Session 3 - 11/30/2024 - 23 packets
[Download](#)

[Back To Dashboard](#)



K9

Summary





K9 Summary

The K9 Packet Sniffer is a robust, user-friendly tool designed to monitor and analyze network traffic. It is targeted at IT professionals, network engineers, cybersecurity specialists, and even casual users seeking to efficiently secure their networks. While tools like Wireshark are widely used, K9 addresses their limitations by prioritizing user-friendliness, secure organization, and streamlined workflows.

Key features of K9 Packet Sniffer include:

- ❖ Open Source: Accessible to a broad audience with continuous enhancements.
- ❖ Simplified Workflows: Offers a secure portal with user authentication for reviewing, managing, and downloading packet capture sessions in one place, eliminating the disorganized downloads common with other tools.
- ❖ Efficient Network Monitoring: Enables users to easily capture and monitor local network traffic.
- ❖ Enhanced Security: Focuses on securely storing packet captures to safeguard sensitive data.

With the release of K9 Packet Sniffer, the tool combines powerful functionality, simplicity, and security, making it easier and more efficient to diagnose network issues, enhance security, and explore traffic. The video concludes with an invitation to experience the upgraded features of the tool.

Contact Info:

- ❖ Edward Medina
➤ emedi074@fiu.edu
- ❖ Maritza Medina
➤ mmedi185@fiu.edu
- ❖ Sharek Rendon
➤ srend011@fiu.edu
- ❖ Tiago Muller
➤ tmull025@fiu.edu
- ❖ Carlos Imery
➤ cimer001@fiu.edu