giv eme a few project ideas that I can build in 2 weeks as IT support specialist or Jr Penetration tester

Here are a few project ideas you can build in approximately two weeks, tailored for someone with an IT support specialist background or aspiring to be a Junior Penetration Tester, drawing on the provided sources and our conversation history:

Project Ideas for an IT Support Specialist:

- Develop an Automated System Health Check Script: As an IT Support Specialist, you are involved in keeping an eye on systems to spot problems early. You can leverage scripting skills, particularly Python which is prevalent and easy to learn, or PowerShell, to create a script that automatically checks the status of critical system components (e.g., disk space, CPU usage, network connectivity, antivirus status). This project will help you automate repetitive tasks and proactively identify potential issues. You could then document how to schedule this script to run regularly.
- Create a Basic Cybersecurity Awareness Training Module: Based on the importance of cybersecurity awareness, you could design a short training module for end-users. This could cover topics like strong passwords, identifying phishing emails [our conversation history], and the importance of installing only approved software. You could use presentation software or a simple document format. This project utilizes your understanding of common security issues and enhances your communication skills by explaining technical concepts to non-technical users.
- Implement and Document a Basic Network Security Policy: Drawing on your understanding of network security, you can draft a basic network security policy for a small hypothetical business. This could include guidelines on password complexity, acceptable use of the network, and procedures for reporting security incidents. You would also document the steps to implement some of these policies, such as enabling password protection on devices and ensuring antivirus software is installed. This project helps you understand security policies and their practical implementation.
- Set Up and Document a Secure Backup and Recovery Process: IT Support Specialists are involved in recovering lost data and ensuring backups. You can set up a simple backup solution for a personal or test

environment and document the entire process, including scheduling backups, verifying their integrity, and performing a test restore. This demonstrates your understanding of data protection and recovery, a crucial aspect of cybersecurity.

Project Ideas for an Aspiring Junior Penetration Tester:

- Build a Basic Vulnerability Scanner using Scripting: Using Python, you can create a simple script that scans a target network or host for open ports or identifies the versions of running services. While not a comprehensive vulnerability scanner, this project will introduce you to the fundamentals of network scanning and vulnerability identification, which are key skills for penetration testing. You can then research common vulnerabilities associated with the identified open ports or service versions.
- Practice Web Application Security Basics on a Lab Environment: Utilize platforms like TryHackMe or OWASP Juice Shop (which you can set up locally) to practice identifying and exploiting common web application vulnerabilities (e.g., cross-site scripting (XSS), SQL injection). Document the vulnerabilities you find, the methods you used to exploit them, and potential remediation steps. This provides hands-on experience in offensive security testing.
- Conduct Open-Source Intelligence (OSINT) Gathering on a Target: Choose a publicly known organization or a safe target (with permission) and practice gathering information using publicly available resources (e.g., search engines, social media, public records). Document the types of information you can find and how this information could potentially be used in a penetration testing scenario. This project highlights the importance of information gathering in security assessments.
- Analyze Network Traffic using Wireshark: Learn to capture and analyze network traffic using Wireshark (a free tool). Focus on identifying different protocols, understanding the communication flow, and looking for any potentially suspicious patterns. You can analyze traffic generated by your own virtual machines or a controlled test environment. This project helps you develop an understanding of network communications, which is essential for both understanding attacks and identifying vulnerabilities.

When choosing a project, consider your current skill set and interests. The Microsoft Cybersecurity Analyst Professional Certificate and the Google Cybersecurity Professional Certificate mentioned in the sources emphasize gaining hands-on experience, so these projects align with that goal. Remember to document your work thoroughly, as this is a key aspect of both IT support and security analysis. Good luck!