Capstone Project Deliverables

Title of the Project: Wyrm: Offline AI Reconnaissance and Hacking Tool
Student Names: Richard Flores, Natasha Menon, and Charles "Matt" Penn
Course: IT 489 B Capstone Project
Institution: Marymount University, College of BILT, School of Technology & Innovation
Date: May 2nd, 2025

Summary

This project consists of an offline hacking & reconnaissance tool enhanced by AI, as well as having bluetooth connection capabilities, which we call Wyrm. The tool is run off of a Raspberry Pi 5's, which is used not only as a mobile device, but also its capability of running multiple operating systems. Reconnaissance, weaponization, and delivery were the main criteria for the tools installed onto the device. Additionally, a local Ollama LLM was chosen to enhance the use of the tools by providing guidance on flags and commands. All code is packaged within a GitHub repository found here. The significance of this project is to determine whether a comprehensive mobile red team device can provide red team operators ease of use, persistence, and efficiency while simulating an attack.

Objectives

This project aims to address this gap by exploring potential solutions and developing a prototype tool that would allow on-site cybersecurity offensive testers to implement at a minimum the first three stages of Lockheed Martin's Cyber Kill Chain by conducting reconnaissance, weaponization, and delivery, with exploitation and installation being an optimal outcome as well, while onsite and attempting to avoid discovery. We have implemented or researched the following:

- To research existing cyber-Linux distributions and tools to identify related gaps.
- To research and identify hacking software tools that are designed for or have effective use cases and capabilities where internet access is not guaranteed.
- To develop scripts or programs to automate common tasks, such as stealthy network scanning, while providing opportunities to customize and run as needed.
- To identify areas where AI could supplement the analysis or decision-making process, reducing time on target during a red team engagement.
- To research and identify methods for user interaction with the solution.
- To research and identify available hardware that satisfies need for a small footprint, such as available Single Board Computer (SBC) solutions and add-on hardware.
- To develop a custom Linux distribution that includes identified tools and scripts.
- To assemble and test a physical prototype as proof of concept.

Github

The Github repository includes the following: tool and package install script for a VM or Raspberry Pi, bluetooth terminal client and target connection scripts, and a folder containing the installation script for the Ollama model, manual pages script, and a main.py file to give instructions to the LLM. More information can be found in the README file in the main Github repository page.

WyrmTerm Bluetooth Scripts

The purpose of the bluetooth scripts are to provide a wireless connection to the Wyrm Raspberry Pi from another client device. This would allow an operator to access the Raspberry Pi semi-remotely using wireless while attempting to avoid detection if WiFi scanning is being conducted. The first script is the WyrmTermTarget.sh script, which runs on the target device to accept Bluetooth serial connections from a client. It customizes the Bluetooth service to advertise a virtual serial port bound to the physical Bluetooth adapter. Getty is then bound to this virtual serial port to allow authenticated terminal logins over Bluetooth. This The second script for bluetooth setup is the WyrmTermClient.sh script. It runs on the client device to initiate a Bluetooth serial terminal connection to a remote target. Similar to the target script, it binds a virtual serial port to physical Bluetooth device, but this time binds a terminal emulator to the virtual port allowing connection to the target device’s MAC address and access to a terminal session. The demonstration of both scripts can be found in the “WyrmTermDemo” video.

WyrmAI LLM Scripts

The AI we chose is a local Qwen2.5-coder through Ollama, an open source platform for installing and using LLMs. The purpose of the AI is to provide guidance and CLI commands for various installed tools, using the documentation and manual pages for each as a reference. The first script run for the WyrmAI is install.sh, which installs the AI hacking assistant and its dependencies in a dedicated directory. It installs Ollama if not already present, installs Python3, pip, and venv system packages, copies project files to /opt/wyrmai/, sets up a Python virtual environment and installs Python dependencies from requirements.txt, and creates a system-wide command wyrmai available from anywhere, which runs the main AI assistant. Next is pull_manpages.sh which extracts and saves documentation for a wide range of security and hacking tools. It creates a manpages directory, iterates through a list of common tools, saving their documentation output to individual text files, and supports fallbacks to –help or -h if man pages are unavailable. The last file is main.py, which is the core Python script for the offline AI hacking assistant. It uses Ollama and ChromaDB to provide AI-powered command suggestions and documentation retrieval, processes and stores Linux manual pages for offline use, and supports interactive chat, single-query mode, and session history review.

Setup Script

The setuptools.sh script is run with sudo permissions and orchestrates the installation of tools and their dependencies. The demonstration video named “WyrmAI_Install_AI.mov” shows the installation process with the script running and is on a VM rather than the Raspberry Pi because of the lack of screen recording tools. It runs not only the tools, but also the processes and dependencies for bluetooth connection and WyrmAI. The following list shows the installed tools in the setuptools.sh script within the Cyber Kill Chain criteria, as well as password cracking:

- Reconnaissance
    - Tshark
    - Searchsploit
    - ARP-Scan
    - Nmap
    - SQLMap
    - GVM CLI
    - Social Engineering Toolkit
    - Aircrack-ng
    - Scapy
    - Snaffler
    - Kismet
- Cracking
    - John The Ripper
    - Responder
    - Hydra
- Weaponization
    - MSFvenom
    - Veil
    - Scarecrow
    - Freeze
- Delivery
    - Metasploit
    - Netcat

Conclusion

Overall, we were able to create a prototype for an offline, AI enhanced reconnaissance hacking tool. We accomplished this by configuring a Raspberry Pi 5, writing a script to install reconnaissance, weaponization, and delivery tools, developing a local AI model to provide guidance to operators, and bluetooth serial terminal connection for less discoverable operations.