BXCI Automations Script - Project Walkthrough

Overview

BXCI Automations is a multifunctional Bash script developed to simplify common cybersecurity and information gathering tasks. The tool includes modules for brute forcing, OSINT, decoding, ZIP file cracking, metadata extraction, and more-all through a user-friendly menu system.

Main Menu

The script launches with a menu-driven interface offering 8 core modules:

1. Info Gathering
2. Brute Force
3. Metadata Extraction
4. OSINT Tools
5. ZIP Cracking
6. Data Breach Tools
7. All-in-One Decoder
8. Exit

All-in-One Decoder

This module accepts either manual input or a file input of an encoded string, then attempts to decode it using several methods: Base64, Hex, Binary, ROT13, and Base32. Each decoding attempt is shown in order.

Data Breach Tools

Two options are offered:

1. Use h8mail to check for leaked credentials (saved to a log file).
2. Open haveibeenpwned.com in the default browser for manual checks.

BXCI Automations Script - Project Walkthrough

ZIP/RAR/7z Cracking

This module automates the password cracking process for compressed archives using tools like john, rar2john, and 7z2john. It extracts hashes and attempts to crack passwords, saving the result in text files.

Metadata Extraction

Provides three tools:

1. ExifTool for metadata.

2. Strings extraction from binary.

3. Binwalk for discovering hidden data in files. Outputs are saved in uniquely named files.

OSINT Tools

A full OSINT suite using:

1. theHarvester for emails and usernames

2. H8mail for credential leaks

3. Wayback Machine URL history

4. SpiderFoot for complete recon. Outputs saved locally.

Info Gathering

Classic reconnaissance tools are bundled together:

- Whois

- NsLookup

- Dig

- Subfinder

- DNSRecon

Options 6 and 7 link directly to the Metadata and OSINT modules.

Logging and Error Handling

Output of various tools is saved using `tee` into log files with meaningful names. Error checks are included for missing files, invalid inputs, and nonexistent tools.