

Table of Contents

Onion C2 Implementation - Part II: Advanced Features

Theory & Foundation

01 Introduction

Advanced Onion C2 implementation overview and ethical considerations

02 Next Steps & Future Vision

Roadmap for web dashboard, multi-platform support, and AI capabilities

03 Project Goals & Open Source

Final objectives and community collaboration approach

04 Onion C2 Analysis

Advantages, disadvantages, and operational trade-offs

Core Implementation Techniques

05 Online Database Integration

MongoDB Atlas setup and remote database connectivity

06 Victim Check-in System

System fingerprinting, registration, and persistent identification

07 Endpoint Protection

IP whitelisting and UUID-based authentication layers

08 Command Execution Pipeline

Complete command workflow with status tracking and output capture

09 Encrypted Communications

AES-256 implementation for secure C2 channel protection

10 Failover Logic

Domain redundancy and infrastructure resilience mechanisms

Practical Application

11 File Operations

Upload and download capabilities for data exfiltration

12 Practical Challenge

Web dashboard development exercise for operational management

13 Conclusions

Key achievements, limitations, and future development path
