

Beyond the Reverse Shell

Practical alternatives for red team command channels

THEORY

01 Introduction

Overview of practical alternatives to classic reverse shells for red team operations

02 Theory of the Command Channel

Understanding command channels, their properties, and trade-offs in stealth and reliability

03 Communication Patterns in Red Teaming

Common ways red teams exchange commands and data with implanted agents

TECHNIQUES

04 Typical Reverse Shell

Implementing a C++ reverse shell with socket redirection and process creation

05 Jumping to Blind Shell

Creating a blind shell that executes commands without direct feedback

06 HTTP/S Web Shell

Implementing command execution through HTTP requests and responses

07 DNS Blind Shell

Using DNS queries and responses for stealthy command execution

08 Windows Local IPC Pipes

Leveraging Windows named pipes for inter-process communication and command execution

09 Exercise

Practical challenge for implementing alternative command channels

10 Conclusions

Key takeaways and ethical considerations for red team operations