

Initial Access Frameworks 2025

BadUSB · QR · SVG — red team techniques & blue team defenses

01 Overview & Safety Notice

Module goals, scope, and ethical use disclaimer for authorized environments only.

02 BadUSB Framework

Architecture, core capabilities, usage guide, attack vectors, and Stage-2 modules.

03 QR Malware Framework

Advanced features, configuration & generation workflow, scenarios, and integrations.

04 SVG Malware Framework

Attack techniques (XXE, script execution), server operations, payload generation.

05 Framework Comparison

Side-by-side matrix: vectors, detection difficulty, delivery, persistence, evasion.

06 Defense Strategies

Prevention controls, monitoring & detection methods, and incident response notes.

07 Learning Objectives

What you'll master: vectors, evasion analysis, defensive design, ethical practice.

08 Practical Laboratory Activity

Hands-on exercises in a controlled lab: setup → execution → analysis → reporting.

09 Conclusion & Key Takeaways

Executive summary, strategic implications, and future considerations.

10 Resources & References

Further reading, standards, and tools mentioned throughout the module.