Beyond EIP

spoonm & skape

BlackHat, 2005

Part I

Introduction

Who are we?

What will we discuss?

The exploitation cycle

Pre-exploitation

Exploitation

Post-exploitation

Part II

Exploitation technology

Opty2

Standard XOR

Additive Feedback XOR

Shikata Ga Nai

What are post-exploitation stagers?

Overview

Implementation: reverse stager

Overview

Implementation

Practical use: HTTP tunneling

Pros & cons

Overview

Beyond EIP

spoonm & skape

Pre-Exploitation

- NOP Generation
- Payload Encoding

Post-Exploitation Stagers

- Windows Ordinal Stagers
- PassiveX
- Egghunt

Post-Exploitation Stages

- Library Injection
- Meterpreter
- DispatchNinja

Hunting for eggs with SEH

Beyond EIP

spoonm & skape

Pre-Exploitation

- NOP Generation
- Payload Encoding

Post-Exploitation Stagers

- Windows Ordinal Stagers
- PassiveX
- Egghunt

Post-Exploitation Stages

- Library Injection
- Meterpreter
- DispatchNinja

Hunting for eggs with system calls

Beyond EIP

spoonm & skape

Pre-Exploitation

- NOP Generation
- Payload Encoding

Post-Exploitation Stagers

- Windows Ordinal Stagers
- PassiveX
- Egghunt

Post-Exploitation Stages

- Library Injection
- Meterpreter
- DispatchNinja

What are post-exploitation stages?

Beyond EIP

spoonm & skape

Pre-Exploitation

- NOP Generation
- Payload Encoding

Post-Exploitation Stagers

- Windows Ordinal Stagers
- PassiveX
- Egghunt

Post-Exploitation Stages

- Library Injection
- Meterpreter
- DispatchNinja

Overview

Types of library injection

In-memory library injection on Windows

In-memory library injection on UNIX

Library injection in action: VNC

Overview

Design goals

Communication protocol specification

Client/Server architecture

Extension flexibilities

Beyond EIP

spoonm & skape

Pre-Exploitation

- NOP Generation
- Payload Encoding

Post-Exploitation Stagers

- Windows Ordinal Stagers
- PassiveX
- Egghunt

Post-Exploitation Stages

- Library Injection
- Meterpreter
- DispatchNinja

Meterpreter extensions in action: Stdapi

Beyond EIP

spoonm & skape

Pre-Exploitation
- NOP Generation
- Payload Encoding

Post-Exploitation Stagers
- Windows Ordinal Stagers
- PassiveX
- Egghunt

Post-Exploitation Stages
- Library Injection
- Meterpreter
- DispatchNinja

Beyond EIP

spoonm & skape

Pre-Exploitation

- NOP Generation
- Payload Encoding

Post-Exploitation Stagers

- Windows Ordinal Stagers
- PassiveX
- Egghunt

Post-Exploitation Stages

- Library Injection
- Meterpreter
- DispatchNinja

Cool dN stuff here

Part III

Advanced Post-Exploitation Suites