Beyond EIP

spoonm & skap

Beyond EIP

spoonm & skape

BlackHat, 2005

Beyond EIP

spoonm & skape

Introduction

Exploitation technology

Pre-exploitation Exploitation

Post-exploitation

Part I

Introduction

Who are we?

Beyond EIP

spoonm & skape

Introduction

Exploitation technology

Pre-exploitation Exploitation

Post-exploitation

What will we discuss?

Beyond EIP

spoonm & skape

Introduction

Exploitation technology

Pre-exploitation Exploitation Post-exploitation

The exploitation cycle

Beyond EIP

spoonm & skape

Introduction

Exploitation technology

Pre-exploitation Exploitation Post-exploitation

Pre-exploitation

Beyond EIP

spoonm & skape

Introduction

Exploitation technology

Pre-exploitation

Exploitation Post-exploitation

Exploitation

Beyond EIP

spoonm & skape

Introduction

Exploitation technology

Pre-exploitation

Post-exploitation

Post-exploitation

Beyond EIP

spoonm & skape

Introduction

Exploitation technology

Pre-exploitation

Exploitation

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

Part II

Exploitation technology

Opty2

Beyond EIP

spoonm & skape

Pre-Exploitation

P Generation

load Encoding

Post-Exploitation Stagers

Windows Ordinal Stagers PassiveX Egghunt

Post-Exploitation Stages

Standard XOR

Beyond EIP

spoonm & skape

Pre-Exploitation

NOP Generation

Post-Exploitation Stagers

Windows Ordinal Stagers PassiveX Egghunt

Post-Exploitation Stages

Additive Feedback XOR

Beyond EIP

spoonm & skape

Pre-Exploitation

NOP Generation

Post-Exploitation Stagers

Windows Ordinal Stagers PassiveX Egghunt

Post-Exploitation Stages

Shikata Ga Nai

Beyond EIP

spoonm & skape

Pre-Exploitation

NOP Generation

Post-Exploitation Stagers

Windows Ordinal Stagers PassiveX

Post-Exploitation Stages

Library Injection Meterpreter DispatchNinja

Egghunt

What are post-exploitation stagers?

Beyond EIP

spoonm & skape

Pre-Exploitation NOP Generation

NOP Generation Payload Encoding

Post-Exploitation Stagers

Windows Ordinal Stagers PassiveX

Post-Exploitation Stages

Library Injection Meterpreter DispatchNinja

Egghunt

Overview

Beyond EIP

spoonm & skape

Pre-Exploitation NOP Generation

Payload Encoding

Post-Exploitation Stagers

Windows Ordinal Stager PassiveX

Egghunt

Post-Exploitation Stages

Implementation: reverse stager

Beyond EIP

spoonm & skape

Pre-Exploitation NOP Generation

NOP Generation Payload Encoding

Post-Exploitation Stagers

Windows Ordinal Stager

PassiveX Egghunt

Post-Exploitation Stages

Overview

Beyond EIP

spoonm & skape

Pre-Exploitation NOP Generation

ayload Encoding

Post-Exploitation Stagers

Windows Ordinal Stager

PassiveX Egghunt

Post-Exploitation Stages

Implementation

Beyond EIP

spoonm & skape

Pre-Exploitation NOP Generation

OP Generation

Post-Exploitation Stagers

Windows Ordinal Stagers

PassiveX Egghunt

Post-Exploitation Stages

Practical use: HTTP tunneling

Beyond EIP

spoonm & skape

Pre-Exploitation

NOP Generation

NOP Generation Payload Encoding

Post-Exploitation Stagers

Windows Ordinal Stagers

Egghunt

Post-Exploitation Stages

Pros & cons

Beyond EIP

spoonm & skape

Pre-Exploitation NOP Generation

OP Generation avload Encoding

Post-Exploitation Stagers

Windows Ordinal Stagers

PassiveX Egghunt

Post-Exploitation Stages

Overview

Beyond EIP

spoonm & skape

Pre-Exploitation NOP Generation

IOP Generation avload Encoding

Post-Exploitation Stagers

Windows Ordinal Stagers PassiveX

Post-Exploitation Stages

Hunting for eggs with SEH

Beyond EIP

spoonm & skape

Pre-Exploitation NOP Generation

NOP Generation Payload Encoding

Post-Exploitation Stagers

Windows Ordinal Stagers PassiveX

Post-Exploitation Stages

Hunting for eggs with system calls

Beyond EIP

spoonm & skape

Pre-Exploitation NOP Generation

NOP Generation Payload Encoding

Post-Exploitation Stagers

Windows Ordinal Stagers PassiveX

Post-Exploitation Stages

What are post-exploitation stages?

Beyond EIP

spoonm & skape

Pre-Exploitation NOP Generation

NOP Generation Payload Encoding

Post-Exploitation Stagers

Windows Ordinal Stagers PassiveX Egghunt

Post-Exploitation Stages

Overview

Beyond EIP

spoonm & skape

Pre-Exploitation NOP Generation

Payload Encoding

Post-Exploitation Stagers

Windows Ordinal Stagers PassiveX Egghunt

Post-Exploitation Stages

Types of library injection

Beyond EIP

spoonm & skape

Pre-Exploitation NOP Generation

NOP Generation Payload Encoding

Post-Exploitation Stagers

Windows Ordinal Stagers PassiveX Egghunt

Post-Exploitation Stages

In-memory library injection on Windows

Beyond EIP

spoonm & skape

Pre-Exploitation NOP Generation

NOP Generation Payload Encoding

Post-Exploitation Stagers

Windows Ordinal Stagers PassiveX Egghunt

Post-Exploitation Stages

In-memory library injection on UNIX

Beyond EIP

spoonm & skape

Pre-Exploitation NOP Generation

NOP Generation Payload Encoding

Post-Exploitation Stagers

Windows Ordinal Stagers PassiveX Egghunt

Post-Exploitation Stages

Library injection in action: VNC

Beyond EIP

spoonm & skape

Pre-Exploitation NOP Generation

NOP Generation Payload Encoding

Post-Exploitation Stagers

Windows Ordinal Stagers PassiveX Egghunt

Post-Exploitation Stages

Overview

Beyond EIP

spoonm & skape

Pre-Exploitation NOP Generation

NOP Generation Payload Encoding

Post-Exploitation Stagers

Windows Ordinal Stagers PassiveX Egghunt

Post-Exploitation Stages

Library Injection

Design goals

Beyond EIP

spoonm & skape

Pre-Exploitation NOP Generation

IOP Generation ayload Encoding

Post-Exploitation Stagers

Windows Ordinal Stagers PassiveX Egghunt

Post-Exploitation Stages

Library Injection

Communication protocol specification

Beyond EIP

spoonm & skape

Pre-Exploitation NOP Generation

NOP Generation Payload Encoding

Post-Exploitation Stagers

Windows Ordinal Stagers PassiveX Egghunt

Post-Exploitation Stages

Library Injection

Client/Server architecture

Beyond EIP

spoonm & skape

Pre-Exploitation NOP Generation

NOP Generation Payload Encoding

Post-Exploitation Stagers

Windows Ordinal Stagers PassiveX Egghunt

Post-Exploitation Stages

Library Injection

Extension flexibilities

Beyond EIP

spoonm & skape

Pre-Exploitation NOP Generation

NOP Generation Payload Encoding

Post-Exploitation Stagers

Windows Ordinal Stagers PassiveX Egghunt

Post-Exploitation Stages

Library Injection

Meterpreter extensions in action: Stdapi

Beyond EIP

spoonm & skape

Pre-Exploitation NOP Generation

NOP Generation Payload Encoding

Post-Exploitation Stagers

Windows Ordinal Stagers PassiveX Egghunt

Post-Exploitation Stages

Library Injection

Cool dN stuff here

Beyond EIP

spoonm & skape

Pre-Exploitation NOP Generation

NOP Generation Payload Encoding

Post-Exploitation Stagers

Windows Ordinal Stagers PassiveX Egghunt

Post-Exploitation Stages

Library Injection Meterpreter Beyond EIP

spoonm & skap

Part III

Advanced Post-Exploitation Suites