Immunity Debugger

1004-P

📜 خطة دورة تدريبية لـImmunity Debugger
🗓️ المدة: 4 أسابيع (مستوى مبتدئ إلى متقدم)

Main Branch: United building – E Shams –Front NBE , El Siouf _Alexandria
Tel: **01102060500-01144470856**

الفرع الرئيسي :عمارات المتحدة – عمارة عين شمس – امام البنك الاهلي – السيوف- الاسكندرية
تليفون: 01102060500 - 01144470856

E-mail. adelramadan@eotss-academy.com
info@eotss-academy.com

🎯 الهدف: إتقان Immunity Debugger لتحليل الثغرات واستغلالها، خاصة Buffer Overflow.

📌 الأسبوع الأول: الأساسيات
✅ مقدمة إلى Immunity Debugger ولماذا يستخدم.
✅ فهم سجلات المعالج (EIP, ESP, EBP).
✅ كيفية تحميل البرامج وتحليلها داخل Immunity Debugger.
✅ تجربة إيقاف نقطة تنفيذ (Breakpoint) وتتبع التعليمات البرمجية.

📖 تمرين عملي: تحليل برنامج بسيط داخل Immunity Debugger.

📌 الأسبوع الثاني: تحليل Buffer Overflow
✅ استغلال Stack-Based Buffer Overflow باستخدام Immunity.
✅ استخدام pattern_create & pattern_offset من Metasploit لتحديد الإزاحة.
✅ التحكم في EIP وإعادة توجيه التدفق إلى Shellcode.

📖 تمرين عملي: تنفيذ استغلال Buffer Overflow على تطبيق ضعيف.

📌 الأسبوع الثالث: استغلال الثغرات باستخدام Shellcode
✅ فهم Shellcode وكيفية استخدامه داخل الاستغلال.
✅ توليد Shellcode باستخدام msfvenom.
✅ تجاوز الحمايات مثل DEP و ASLR.

📖 تمرين عملي: إنشاء Shellcode مخصص واستغلال التطبيق عبر Reverse Shell.

📌 الأسبوع الرابع: تحديات متقدمة وتحليل الثغرات الحقيقية
✅ تحليل ثغرات حقيقية مثل CVE-2017-5638.
✅ التعرف على تقنيات ROP (Return-Oriented Programming).
✅ استخدام Immunity Debugger مع mona.py! لتطوير استغلالات أكثر تعقيدًا.

📖 تمرين عملي: استغلال ثغرة حقيقية في تطبيق Windows.

🎯 ماذا ستتعلم في هذه الدورة؟

✓القدرة على تحليل البرامج داخل Immunity Debugger.
✓تنفيذ هجمات Buffer Overflow خطوة بخطوة.
✓كتابة Shellcode مخصص وتجاوز الحمايات الحديثة.
✓اكتساب مهارات متقدمة في استغلال الثغرات الأمنية.

Code: 1004-P

📜 Training Plan for Immunity Debugger
🗓️ Duration: 4 weeks (Beginner to Advanced Level)
🎯 Goal: Master Immunity Debugger for vulnerability analysis and exploitation, particularly Buffer Overflow.

📌 Week 1: The Basics
✅ Introduction to Immunity Debugger and its purpose.
✅ Understanding processor registers (EIP, ESP, EBP).
✅ Loading and analyzing programs inside Immunity Debugger.
✅ Setting breakpoints and stepping through code execution.

📖 Practical Exercise: Analyzing a simple program in Immunity Debugger.

📌 Week 2: Buffer Overflow Analysis
✅ Exploiting Stack-Based Buffer Overflow using Immunity.
✅ Using pattern_create & pattern_offset from Metasploit to determine offsets.
✅ Controlling EIP and redirecting execution flow to Shellcode.

📖 Practical Exercise: Exploiting a Buffer Overflow vulnerability in a weak application.

📌 Week 3: Exploiting Vulnerabilities with Shellcode
✅ Understanding Shellcode and its role in exploitation.
✅ Generating Shellcode using msfvenom.
✅ Bypassing protections like DEP and ASLR.

📖 Practical Exercise: Creating custom Shellcode and exploiting an application via Reverse Shell.

📌 Week 4: Advanced Challenges and Real-World Exploits
✅ Analyzing real-world vulnerabilities like CVE-2017-5638.
✅ Learning ROP (Return-Oriented Programming) techniques.
✅ Using Immunity Debugger with !mona.py for advanced exploit development.

📖 Practical Exercise: Exploiting a real-world Windows application vulnerability.

🎯 What Will You Learn in This Course?
✓ Ability to analyze programs inside Immunity Debugger.
✓ Step-by-step Buffer Overflow exploitation.
✓ Writing custom Shellcode and bypassing modern protections.
✓ Gaining advanced skills in vulnerability exploitation.

Edite By: Dr. Eng. Adel Ramadan