Exploiting and Defense

Dobin Rutishauser

December 2016

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Intro

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

About Me

Dobin Rutishauser

Working as Security Analyst @ Compass Security

- Penetration Tests
- Webapp Checks
- Architecture Reviews
- & lots more

Interested in ~~Hacking~~ Security since I was little (1999+)

Compass

Compass Security

Ethical Hacking & Incident Response

Compass Security ist ein auf Security Assessments und forensische Untersuchungen spezialisiertes Unternehmen. Wir führen sowohl Penetration Tests als auch Security Reviews durch und unterstützen bei der Koordination und Analyse von Vorfällen.

Penetration Tests

Als Angreifer untersuchen wir Geräte, Netze, Dienste und Anwendungen auf Schwachstellen. Mittels Social Engineering und Red Teaming testen wir das Verhalten der gesamten Organisation. » **weiterlesen**

Security Reviews

Erfahrene IT Analysten unterstützen Sie mit Zweitmeinungen zu Security-Konzepten und prüfen nach Wunsch den Aufbau, die Konfiguration und den Quellcode Ihrer Lösung. » **weiterlesen**

Digital Forensics

Unsere Forensik-Experten helfen bei der Koordination von Vorfällen und Sofortmassnahmen sowie bei der gerichtsfesten Bearbeitung von Daten. Zudem bieten wir eine unkomplizierte und schnelle Ursachenforschung. » **weiterlesen**

Security Trainings

Profitieren auch Sie vom Wissen unserer Analysten zu Penetration Testing, Netzwerkanalyse, sichere Apps und Anwendungen, Digitale Forensik und trainieren Sie in einem eigens dafür erstellten Labor. » **weiterlesen**

FileBox

FileBox ist eine Secure File Transfer und Secure Storage Lösung. Damit haben Sie die Möglichkeit, Dokumente sicher auszutauschen. » **weiterlesen**

Hacking-Lab

Hacking-Lab ist eine Online-Plattform für Ethical Hacking, Netzwerke und IT Sicherheit, die sich der Suche und Ausbildung von Cyber Security Talenten widmet. » **weiterlesen**

Compass is hiring (always)

Wir haben verschiedene Stellen als **Penetration Tester** aber auch als **Software Entwickler** offen und würden uns sehr über Deine **Bewerbung** freuen.

Bist Du grundsätzlich vom Typ "Grübler" und "Tüftler"? Hast Du Freude daran, Dich in neue Themen und Techniken einzuarbeiten? Dann bist Du bei Compass genau richtig!

Bitte schicke Deine Fragen an ivan.buetler@compass-security.com und Deine offizielle Bewerbung an hr@compass-security.com

Gruss Ivan Bütler, E1

I got a bit overboard when I was little

Vorlesung

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Vorlesung

Websites:

https://exploit.courses

- Online exploit development website
- Uses Hacking-Lab accounts

https://www.hacking-lab.com

- Half-online challenges website


Siiiii abr ähhhhhh
EBP isch doch 32 bit?
shutterstock
IMAGE ID: 120482521
www.shutterstock.com

Motivation

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch


Looking behind
the curtain

Motivation

For the computer enthusiast:

- How do functions work?
- How does the memory allocator work?
- Whats the difference between userspace and kernelspace?
- How does computer work?

For the hacker:

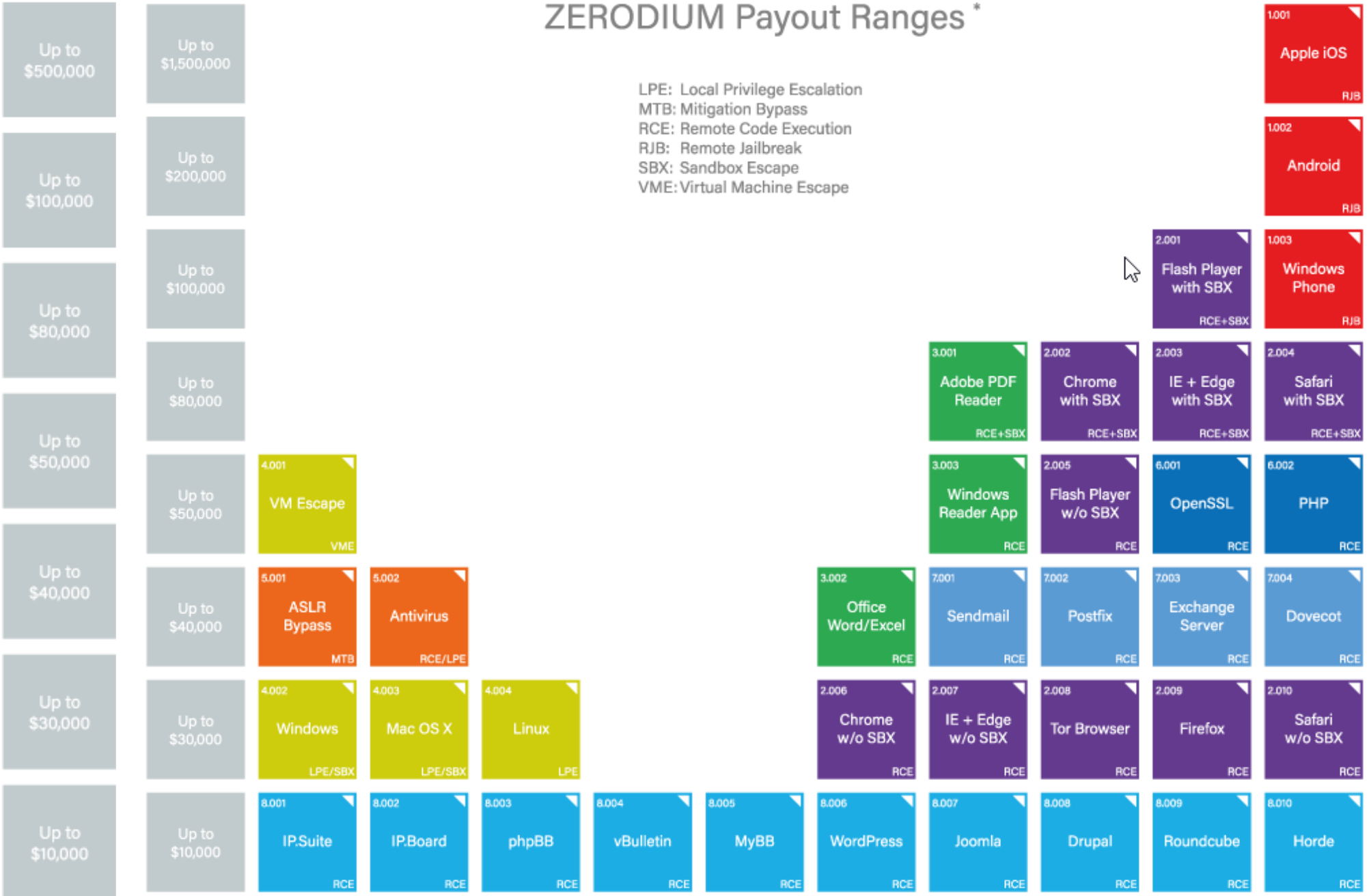
- Develop exploits
- Debugging of C/C++ code
- Being 31337

For the future CISO:

- Assess CVSS score for vulnerabilities
- Assess security mitigations
- Better risk analysis

ZERODIUM Payout Ranges *

LPE: Local Privilege Escalation
MTB: Mitigation Bypass
RCE: Remote Code Execution
RJB: Remote Jailbreak
SBX: Sandbox Escape
VME: Virtual Machine Escape



* All payout ar

* All payout amounts are chosen at the discretion of ZERODIUM and are subject to change or cancellation without notice.

Content of the next 7 Friday afternoons

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

You want to learn:

- What memory corruptions are
- What buffer overflows are
- What exploits are
- How exploits are being created
- To exploit a local application
- To exploit a remote application
- Learn about anti-exploiting technologies
- To circumvent all common anti-exploiting technologies for Linux
- And some for Windows
- Use After Free
- Hack browsers
- Hack facebook “for a friend”

You will actually learn:

- Intel x86
  - Architecture
  - CPU
  - Registers
- Linux
  - Userspace memory layout, stacks, heap
  - Syscalls
  - Sockets
  - Networking
- Programming Languages
  - Assembler
  - C
  - Python
  - Bash
  - (Ruby)

Plan

24.02.2017

Theory:

- 0x01 Intro (this)
- 0x02 Intro Technical
- 0x10 Intel Architecture
- 0x11 Memory Layout

Challenges:

- 0 Introduction to memory layout – basic
- 1 Introduction to memory layout - advanced

Plan

03.03.2017

Theory:

- 0x12 C Array and Pointers
- 0x30 ASM Intro
- 0x31 Shellcode
- 0x32 Function Call Convention
- 0x33 Debugging

Challenges:

- Challenge 8
- Challenge 9
- Challenge 3
- Challenge 7
- Challenge 50

Plan

10.04.2017

Theory:

- 0x41 Buffer Overflow
- 0x42 Exploit
- 0x44 Remote Exploit

Challenges:

- Challenge11
- Challenge12

Plan

17.04.2017

Theory:

- 0x51 Exploit Mitigation
- 0x52 Defeat Exploit Mitigation
- 0x53 Exploit Mitigation – PIE
- 0x54 Defeat Exploit Mitigation ROP

Challenges:

- Challenge14
- Challenge15

Plan

24.04.2017

Theory:

- 0x72 Linux Hardening
- Defeat Exploit Mitigation – Heap Intro
- Defeat Exploit Mitigation – Heap Attacks

Challenges:

- Challenge31

Plan

31.04.2017

Theory:

- Windows Exploiting
- Secure Coding
- Fuzzing

Challenges:

Plan

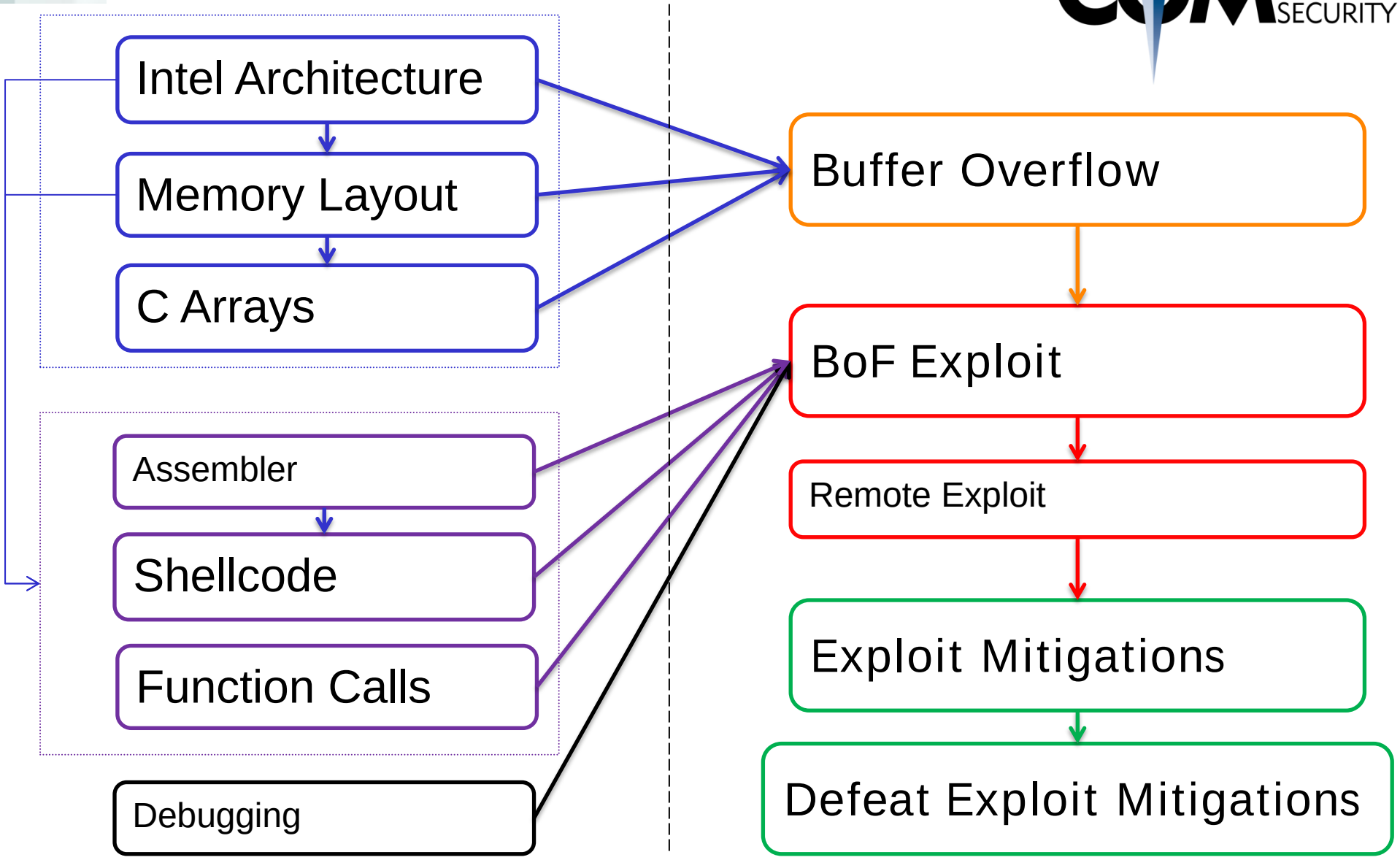
07.05.2017

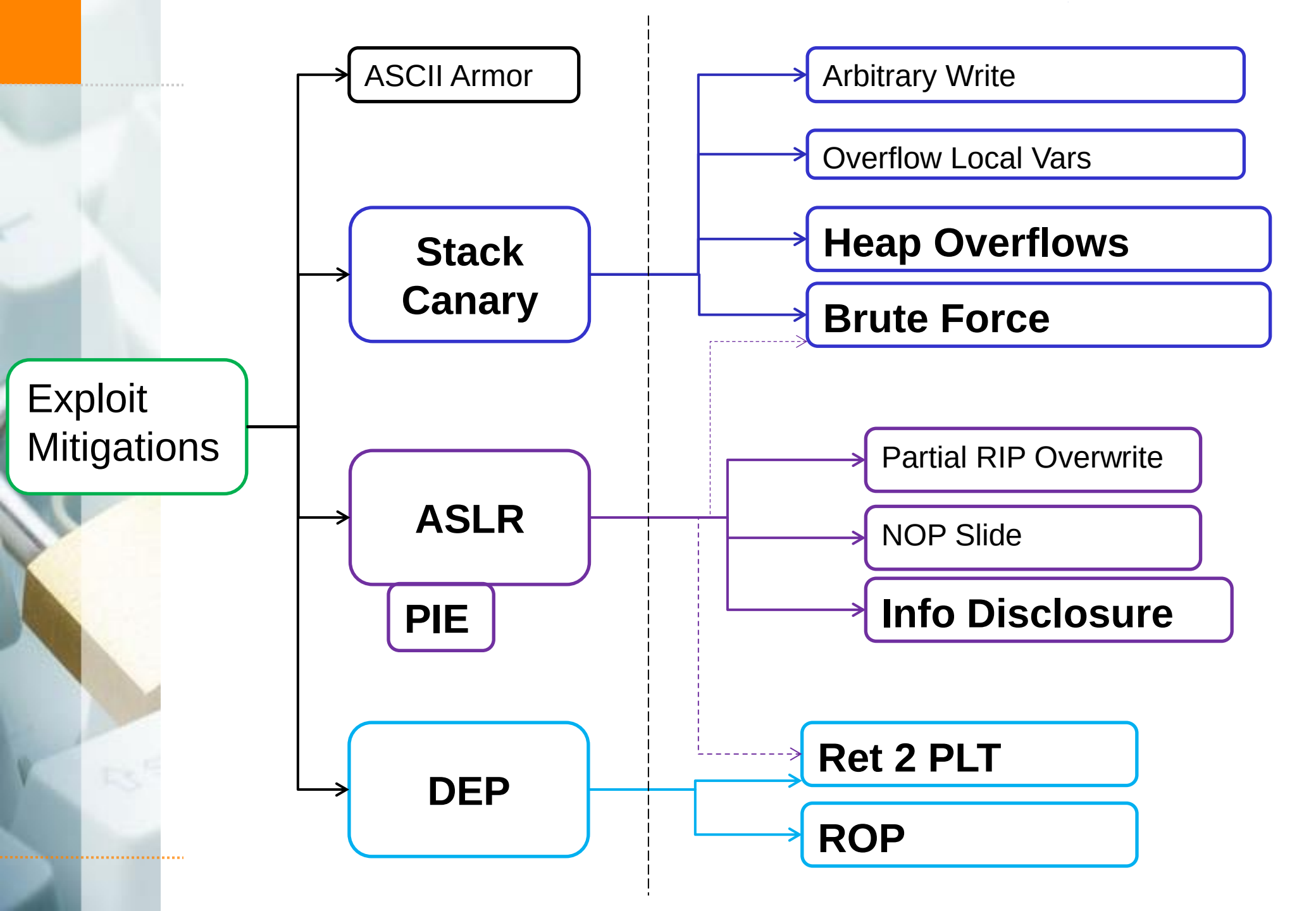
Theory:

- Puffer
- Case Studies
- Questions

Challenges:

Content


Intel Architecture
Memory Layout
C Arrays
Assembler
Shellcode
Function Calls
Debugging
Buffer Overflow
BoF Exploit
Remote Exploit
Exploit Mitigations
Defeat Exploit Mitigations


Exploit Mitigations
ASCII Armor
Stack Canary
ASLR
PIE
DEP
Arbitrary Write
Overflow Local Vars
Heap Overflows
Brute Force
Partial RIP Overwrite
NOP Slide
Info Disclosure
Ret 2 PLT
ROP

And:

Windows Exploiting

Fuzzing

Browser Security

Secure Coding

Linux Hardening

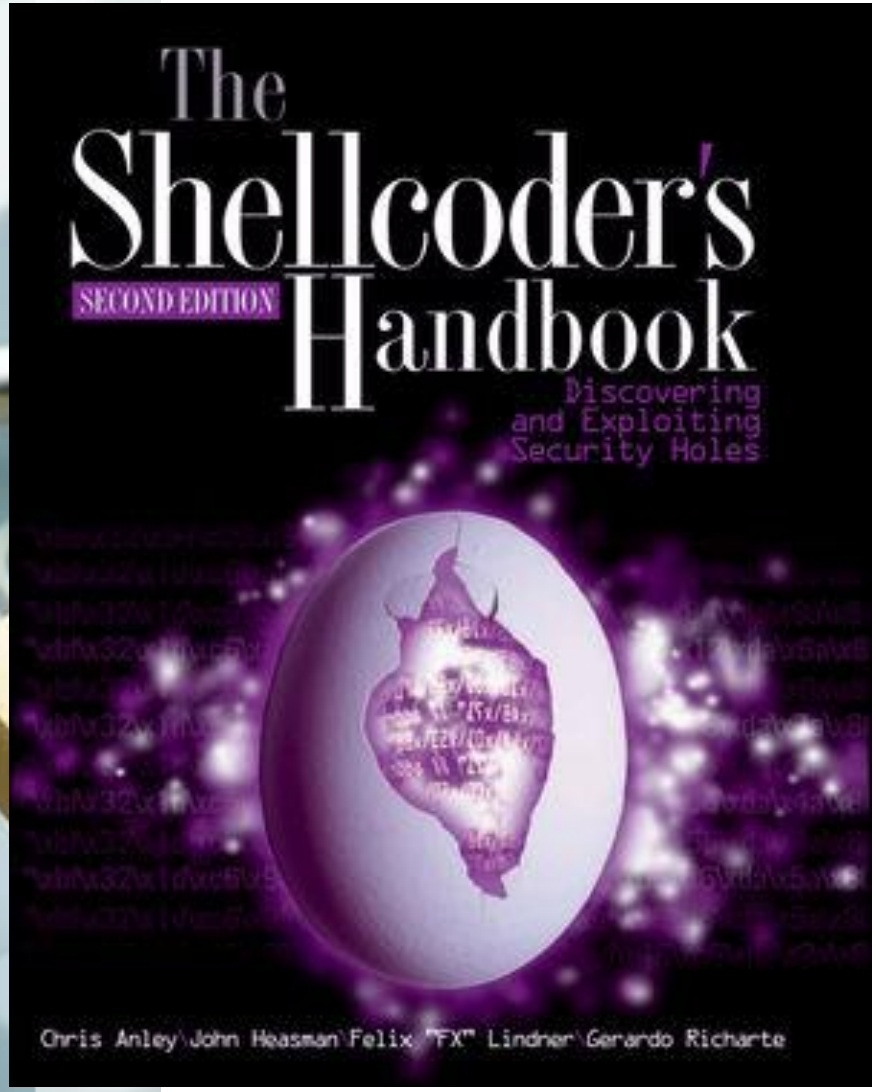
Case Studies

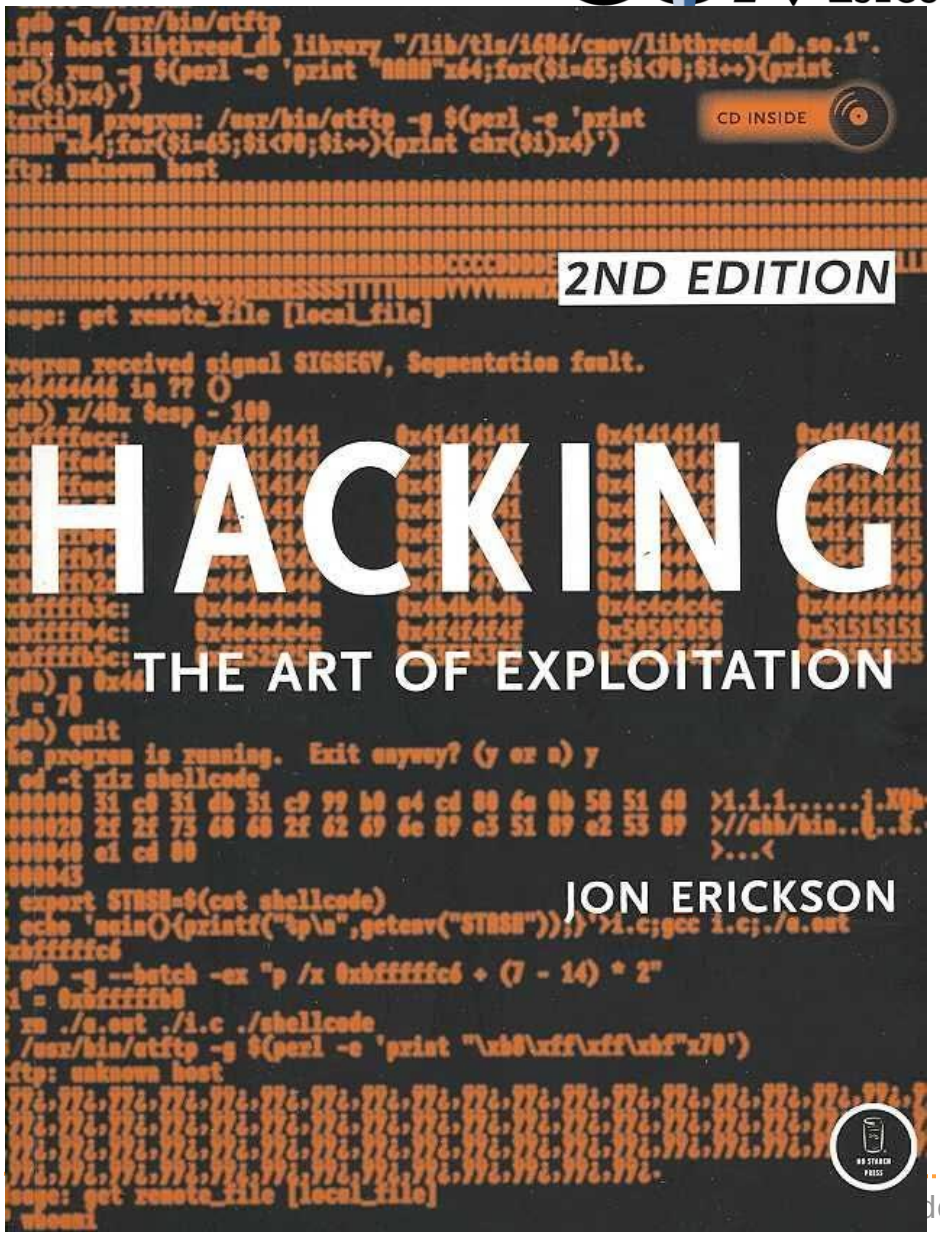
Exam Oral

What is (mainly) relevant for the oral exam?

- How does memory corruption work?
- How does an exploit work?
- What exploit mitigations exist?
- How can these exploit mitigations be circumvented?

Books


The
Shellcoder's
SECOND EDITION
Handbook
Discovering
and Exploiting
Security Holes
Chris Anley\John Heasman\Felix "FX" Lindner\Gerardo Richarte


CD INSIDE
2ND EDITION
HACKING
THE ART OF EXPLOITATION
JON ERICKSON