h_da

HOCHSCHULE DARMSTADT
UNIVERSITY OF APPLIED SCIENCES

The Same, but Different: The Pentesting Study

Jan Roring [1], Dominik Sauer [1], Michael Massoth [1]

[1] Department of Computer Science, University of Applied Sciences Darmstadt

Contact email: jan.roring@stud.h-da.de

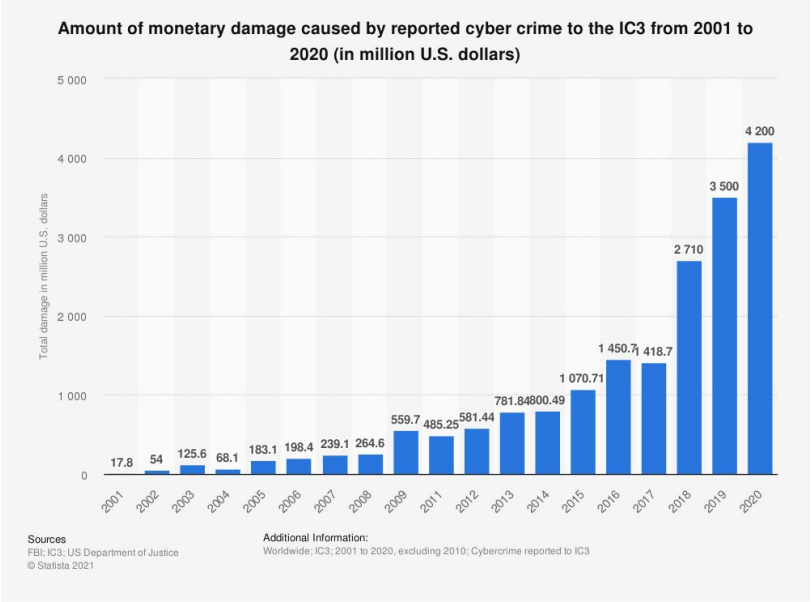
IARIA

Presenter: Jan Roring

- Jan Roring graduated from Darmstadt University of Applied Sciences in 2021 with a master’s degree in computer science majoring in IT security.
- He has been working in IT security since 2017 and began specializing in penetration testing in 2019, after a few years of hacking experience with online capture-the-flags.

Introduction

- Cyber security incidents are on the rise and cause tremendous damage
- To reduce the risk of an incident, companies have the security of their IT systems and applications checked



Introduction

- Penetration testing is a way to identify potential security vulnerabilities
- Through remediation of identified vulnerabilities, customers can improve their security
- Standardized approaches should guarantee reproducible and qualitative results
- Nevertheless, our study shows that the results vary greatly depending on the penetration tester

Penetration Testing

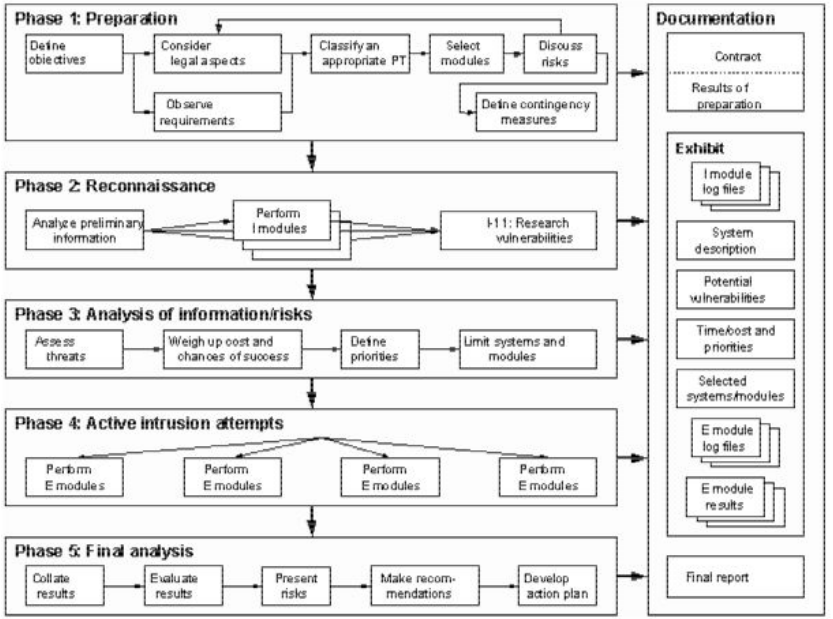
- Simulates attack by a hacker
  - Identification of possible vulnerabilities
  - Proof of existence through exploitation
- Final report for customer
  - List of vulnerabilities
  - Risk Assessment
  - Recommendations
- Aim: Fix vulnerabilities before they are exploited by an attacker

Commonly Used Standards

- Government standards
  - USA: National Institute of Standards and Technology (NIST)
  - Germany: Federal Office for Information Security (BSI)
- Community standards
  - Open Source Security Testing Methodology Manual (OSSTMM)
  - Penetration Testing Execution Standard (PTES)
  - OWASP Web Security Testing Guide

BSI Penetration Testing Model

- Penetration testing methodology consisting of 5 phases
- Uses modules containing test points based on OSSTMM
- Primarily aimed at infrastructure penetration tests



Five-phase penetration testing procedure (A Penetration Testing Model, Federal Office for Information Security, 2003)

OWASP Web Security Testing Guide

Contains test points in categories covering different areas of web applications:

1. Information Gathering
2. Configuration and Deployment Management Testing
3. Identity Management Testing
4. Authentication Testing
5. Authorization Testing
6. Session Management Testing
7. Input Validation Testing
8. Testing for Error Handling
9. Testing for Weak Cryptography
10. Business Logic Testing
11. Client-side Testing
12. API Testing

Penetration Testing Skill Sets

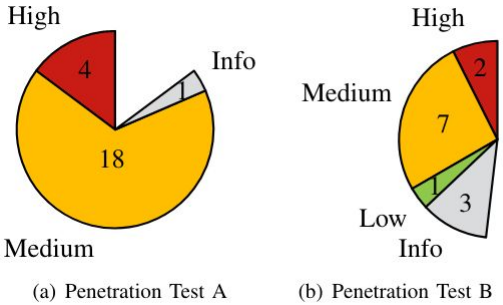
- Hard Skills / Knowledge
  - System administration / operating systems
  - TCP/IP and other network protocols
  - Programming languages
  - IT security products
  - Hacking tools and vulnerability scanners
  - Applications / application systems
- Soft Skills
  - Intuition
  - Creativity

Approach

- Comparison of the results of two web application penetration tests
- Two independent service providers
  - both certified professionals
- Same conditions
  - Four days of testing, one day to create the report
  - Methodology based on OWASP and BSI
  - Same four web applications
- Side-by-side comparison of the findings in the reports

Results

- Reports show some overlap due to the use of similar approaches
- Although covered by the OWASP Testing Guide, one penetration tester overlooked several vulnerabilities
- The results also show that the penetration testers used individual approaches that go beyond the OWASP Testing Guide



(a) Penetration Test A (b) Penetration Test B

Overall vulnerabilities identified by the contractors (grouped by risk potential)

Conclusion

- Standards ≠ guarantee for successful penetration test
- Results can differ significantly despite use of standards
- Human component was decisive factor
- Certifications = proof of hard skills
- Soft skills have huge impact on quality
  - Creativity allows for better results
  - Over-reliance on intuition may lead to false assumptions

Possible Further Research

- Interaction between hard skills and soft skills of penetration testers and their impact on penetration testing results.
- Individual penetration testing approaches and combinations of established standards