Keuzevak Cybersecurity

Linde Nouwen

Karel de Grote Hogeschool

CyberSecurity ReportWriting

Karel de Grote Hogeschool

Professional Conduct

Professional Approach?

- Get permission!
- Agree on what can and cannot be done.
  - scope
  - rules
- If necessary
  - NDA

Professional Approach?

- During hack = keep stakeholders happy by providing short status-reports (email, phonecall, …)
  - Timing should be discussed in advance
  - Use Project Management techniques
  - Methodology/structure should be clear
- Write the report → structure can be “fixed” = see next…
  - Bridge the gap between technical and the business
  - No value until the report is provided
  - Document
    - Method
    - Actions
    - Findings
    - Recommendations

Professional Approach?

- Decide beforehand what is requested:

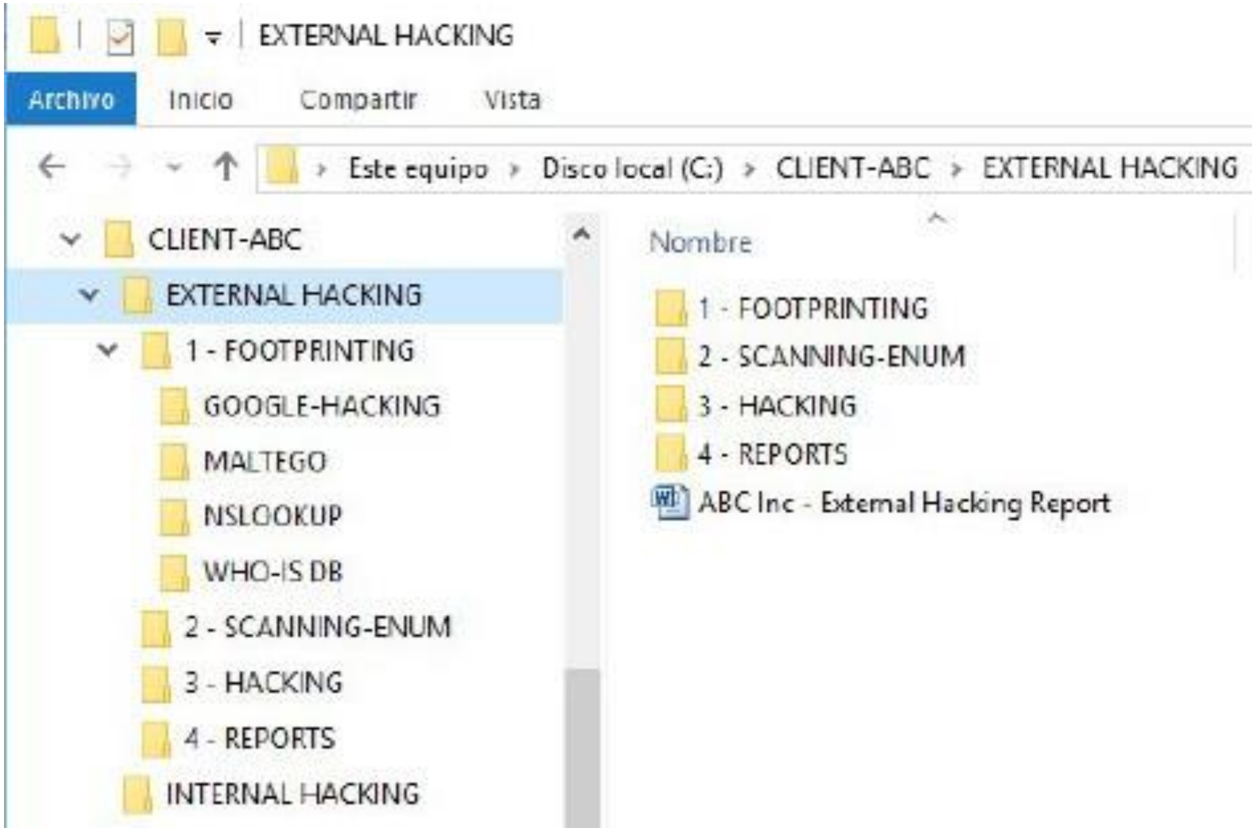
- Presentation of the report to the client
  - This is just what it states; the report is generated and handed over to the client, and if they need any further explanations or discussion they will request it. If no explanation is needed, then the testing and reporting process is complete and the job is finished.
- Presentation plus recommendations
  - If the client requests it, the tester will explain the results of the test and then propose recommendations to fix the problems discovered. The client may not ultimately use all or any of the recommendations, but they will request them to see what needs to be done.
- Presentation plus recommendation with remediation
  - In this particular outcome the test is completed and the review and recommendations are made. What differentiates this outcome from the others is that the client asks the tester to get involved at some level with actually implementing fixes.

During your hacking/testing

- Put everything in one (safe) place (folder + encryption)
- Log console input and output
- Take many screenshots
- Record video (if possible/needed) → tools!
- Take notes (tools: tree-structure & links to gathered information; record findings seperately)
- Keep track of timing (logbook)
- Communicate frequently → see "professional approach"
- Use a report-template
- Use documentation tools

Professional Approach?

- From Karina Astudillo (CEH):


EXTERNAL HACKING
Archivo
Inicio
Compartir
Vista
Este equipo › Disco local (C:) › CLIENT-ABC › EXTERNAL HACKING
Nombre

CLIENT-ABC
EXTERNAL HACKING
1 - FOOTPRINTING
GOOGLE-HACKING
MALTEGO
NSLOOKUP
WHO-IS DB
2 - SCANNING-ENUM
3 - HACKING
4 - REPORTS
INTERNAL HACKING

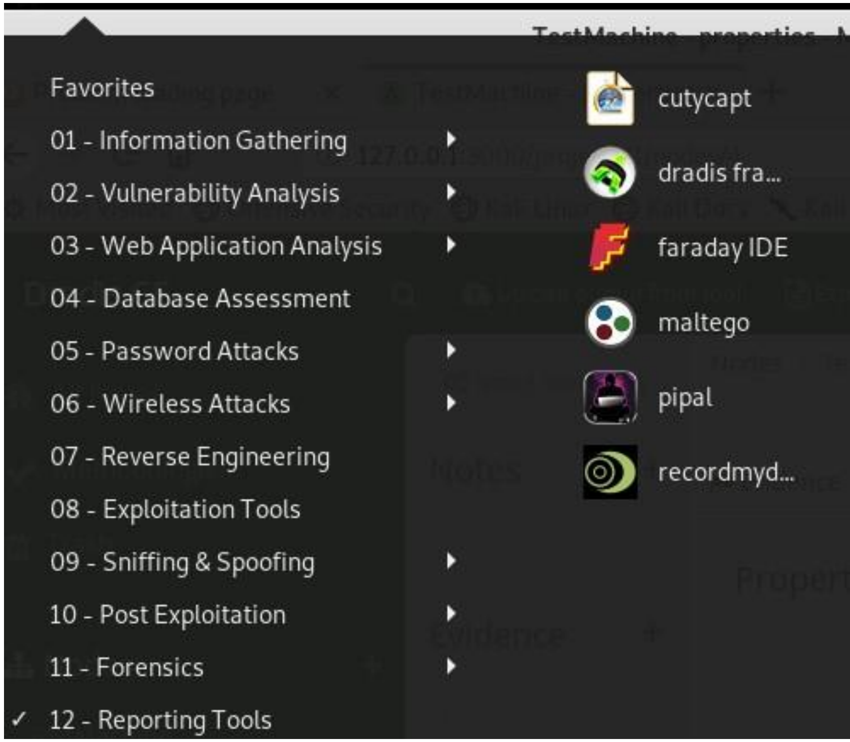
1 - FOOTPRINTING
2 - SCANNING-ENUM
3 - HACKING
4 - REPORTS
ABC Inc - External Hacking Report

Report Writing Techniques

- Write for the audience
  - Executive
  - Middle management
  - Technical experts
- Find a reliable reviewer
- Drafts and several read-throughs
- Concise and simple language
- Leave technical jargon for technical sections

Report Writing Techniques

- Tools/software for “evidence gathering”
  - Dradis (web)
  - MagicTree (desktop)
- Advantages
  - Information stored in database
    - Query
    - Grouping & Association
- Tools are included in KALI:



Report Structure

1. Executive Summary
2. Introduction
3. Target Environment
4. Method Overview
5. Summary of findings
6. Method and Stages
7. Recommendations
8. Conclusion
9. Appendices

Executive Summary

- What was done
- What was found
- What needs to happen
- Overall level of risk
- Top three, top five maximum
- Expect an executive audience
- Five minutes to read
- Absolutely no technical concepts
- Models? (categories, structure, …)

Introduction

- Business perspective for test
- Purpose of test
- Who the test is conducted for
- What the report contains
- The novice reader

Target environment

- Summary description of the target environment
- IP addresses
- DNS names
- Applications
- Internal / external view
- Information provided
- Semi-technical audience

Method Overview

- In context to the scope
- Brief description of stages
- What techniques where used
- Who performed the testing
- Semi-technical audience

Method

- Any frameworks used
- Testing details in stages
  - Stage 1 – OSINT
  - Stage 2 – Enumeration
  - Stage 3 – Vulnerability scanning
  - Stage 4 – Exploitation
  - Stage 5 – Password guessing
  - Stage 6 – Persistence and pivoting
- Plenty of screenshots
- Technical audience

Summary of Findings

- A table of results in order of severity
- Risk details – business context
  - Assets exposed
  - Threat scenarios
  - Difficult or easy to exploit
  - Likelihood of being discovered
  - Recommendations
- Technical audience

Conclusion

- Similar to executive summary
- Details:
  - Findings
  - Timing
  - Success
  - Recommendation summary
- Semi-technical audience

Appendices

- Proof
- Commands and tools
- Replication details
- Output with long length
- Highly technical audience

Providing the Report

- Sensitive information
- Encrypt the report
  - BitLocker (in Windows)
  - Veracrypt (OpenSource)
  - EFS (in Windows)
- Limit distribution
- Never discuss outside of the engagement
- Retesting