Ethical hacking and Penetration Testing

Writing commercial-grade report

Author: Kutlymurat Mambetniyazov (@manfromkz)

Identifying the goals of lesson

- Reviewing commercial-grade report template

Advices

- Always make documentation for findings, including screenshots, exact address, time
- Again, always do screenshots (with maximum information)
- In case of testing serious vulnerabilities (like RCE), even if customer said “that is testing environment”, ask twice
- Make mini draft reports (at least every week), it will easier to merge them to the final report

Structure

- Main conditions, content table
- Methodology
- Scope
- Executive summary
- Detailed information about vulnerabilities
- Remediation
- Appendix

Short rules of report formatting

- Use same fonts and sizes for each element groups
- Numerate each figure, picture, table
- Add indent before and after figures/picture/table etc.
- Text align => “justify”
- Scripts and codes should be in a text box / appendix or separate file
- Keep the formal style

CWE & CVSS & CVE

- https://cwe.mitre.org/ - vulnerabilities category
- https://www.first.org/cvss/ - vulnerabilities impact calc
- https://cve.mitre.org/ - vulnerabilities ids

Pentest report templates

- https://pentestreports.com/reports/
- https://github.com/kutlymurat/pentest_course

Automated reporting tools

- https://vulnrepo.com/
- https://hexway.io/
- https://github.com/pwndoc/pwndoc
- https://github.com/infobyte/faraday

- Online tools for pentest reporting are comfortable, but what if someone will hack them?

Any questions?

Useful links

- https://cobalt.io/blog/how-to-write-an-effective-pentest-report-vulnerability-reports
- https://www.offensive-security.com/pwk-online/PWKv1-REPORT.doc
- https://www.youtube.com/watch?v=EOoBAq6z4Zk
- https://purplesec.us/wp-content/uploads/2019/12/Sample-Penetration-Test-Report-PurpleSec.pdf
- https://www.boisestate.edu/cobe/cobe-writing-style-guide/guidelines-for-reports/