

Security Testing (Introduction)

Martin Stanek

2024

Table of Contents

Course Introduction

Initial thoughts on security testing

Pentesting standards and methodologies

Case studies

Course Introduction

- Security Testing
 - Thursday @ 9:50, room M-V
- Grades
 - 30% be prepared – exercises throughout the semester
 - 30% multiple choice test (at the end of the semester)
 - 40% project: 20 min. presentation (OK, partially, not OK)
- Slides and projects available on the web page
- Contact
 - email: stanek@dcs.fmph.uniba.sk
 - room: M-214
 - web page: www.dcs.fmph.uniba.sk/~stanek

Course topics (tentative)

1. Security Testing (Introduction)
2. Know your enemy
3. Passive Reconnaissance and OSINT
4. Active Reconnaissance
5. Privilege escalation and Pivoting
6. Web and Mobile Application Testing
7. Threat Modeling
8. Vulnerability Scanning and Compliance
9. Social Engineering
10. Red Teaming

Motivation

- compliance (examples):
 - laws (EU regulations – Digital Operational Resilience Act)
 - industry standards (PCI-DSS)
 - 3rd party requirements (SWIFT)
- risk assessment (IT, operational, fraud, etc.)
- assess the security posture or cyber resilience

Vyhláška č. 493/2022 NBÚ o audite kybernetickej bezpečnosti, príloha č.1:

- Minimálne náležitosti žiadosti o vykonanie auditu kybernetickej bezpečnosti
bod 4. *Zoznam informačných systémov a ich klasifikácia s väzbou na základnú službu a pre každý z nich najmenej informácie o informačnom systéme a*

...

h) správa z posledného penetračného testovania informačného systému, použitá metodika a rozsah testovania a doloženie kvalifikácie zamestnancov vykonávajúcich penetračné testy, ak sú penetračné testy vykonané

EU regulation 2022/2554 on digital operational resilience for the financial sector

- *In order to achieve a high level of digital operational resilience . . . financial entities should **regularly test** their ICT systems and staff having ICT-related responsibilities with regard to the effectiveness of their preventive, detection, response and recovery capabilities, to uncover and address potential ICT vulnerabilities.*
- threat-led penetration testing (TLPT)
a framework that mimics the tactics, techniques and procedures of real-life threat actors perceived as posing a genuine cyber threat, that delivers a controlled, bespoke, intelligence-led (red team) test of the financial entity's critical live production systems

PCI DSS 4.0 Requirement 11: Test Security of Systems and Networks Regularly

- 6 sections for this requirement
- informally: processes, wireless access, vulnerabilities, penetration testing, network IDS, file integrity, integrity of payment pages

Swift Customer Security Controls Framework v2023

- 7.3A Penetration testing
Validate the operational security configuration and identify security gaps by performing penetration testing.

Why – the importance of security testing

More practical view

- ensure security controls are working as intended
- security controls have assumptions, verify they (still) hold
- finding gaps in the defense mechanisms, vulnerabilities, weak spots, missing controls
- verify the efficiency of incident detection and response
- assess employees security habits
- *real demonstration of a security problem can be very persuasive*

People & Process & Technology

- software (information systems)
 - often custom web application, mobile application, APIs etc.
- IT infrastructure
 - networks (e.g. DMZ, WLAN, cloud)
 - HW and SW IT components (e.g. network devices, servers, endpoints)
 - services (e.g. such as AD, VoIP, remote access)
- security controls – firewalls, IDS/IPS, AV/EDR¹, access controls, PAM, etc.
- administrative security controls – policies, procedures (incident handling)
- people, e.g. awareness, skills

¹Endpoint Detection and Response

How – different types of security testing

- Software testing
 - (ISO/IEC 25010) System and software quality models
 - security is one of the quality characteristics
 - find vulnerabilities in software (ideally before deployment, part of SDLC)
 - code review, static and dynamic analysis, fuzzing, etc.
- Vulnerability scanning/assessment
 - identify known vulnerabilities in COTS components
 - missing updates, configuration weaknesses
 - automation
 - remove false positives, interpret results

How (cont.)

- Penetration testing
 - simulating an attack on defined target
 - usually a standard methodology is followed
 - testing all relevant vectors
- Red Teaming
 - goal oriented, specific objectives
 - wide range of techniques and their combination
 - single path to success is enough
- Risk assessment
 - high-level assessment of threats and vulnerabilities
 - probability and impact
- Testing design/architecture – threat modeling
- ...

Know/clarify in advance

- internal or external
- white/gray/black-box
- limits, rules, expected outputs

Why, What and How \Rightarrow different techniques, tools, skills, requirements, etc.

Pentesting standards and methodologies

- usually focused more on process than methods and techniques
- some are more useful (e.g. OWASP) than other (e.g. OSSTMM)
- OWASP (Open Web Application Security Project)
 - OWASP Web Security Testing Guide
 - OWASP Mobile Security Testing Guide
- NIST Special Publication 800-115
 - Technical Guide to Information Security Testing and Assessment
- PTES (Penetration Testing Execution Standard) and PTES Technical Guidelines
- PCI Data Security Standard: Penetration Testing Guidance
- OSSTMM (Open Source Security Testing Methodology Manual)
- FedRAMP (Federal Risk and Authorization Management Program)
 - FedRAMP Penetration Test Guidance (focused on cloud providers)

Penetration test – structure

generic

- Pre-engagement
- Reconnaissance/OSINT
- Scanning/Discovery
- Gaining Access
- Maintaining access
- Reporting and Risk Analysis
- Remediation

NIST

- Planing
- Discovery
- Attack (with additional discovery)
- Reporting

PTES

- Pre-engagement Interactions
- Intelligence Gathering
- Threat Modeling
- Vulnerability Analysis
- Exploitation
- Post Exploitation
- Reporting

OWASP WSTG (4.2)

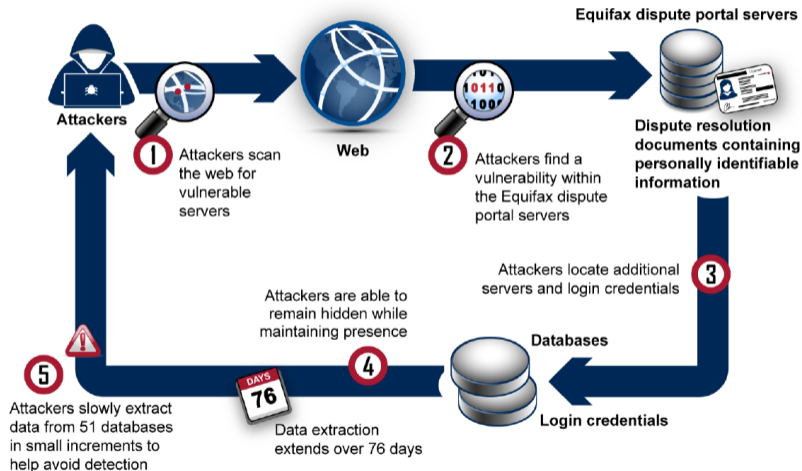
- Information Gathering
- Configuration and Deployment Management Testing
- Identity Management Testing
- Authentication Testing
- Authorization Testing
- Session Management Testing
- Input Validation Testing
- Error Handling
- Cryptography
- Business Logic Testing
- Client-side Testing
- API Testing

Case study 1 – Equifax (2017)

- Equifax – multinational consumer credit reporting agency
 - one of the three largest agencies of this type
 - 25 countries, 13000 employees
- vulnerability in Apache Struts Web Framework (published in March 2017)
- the attack lasted for 76 days (undetected)
- personal data of nearly 150 million people stolen
- GAO report [1] and Congressional report [2]
 - one of few detailed account of a high-profile breach
 - not just vulnerability and patching

Equifax – what happened

How Attackers Exploited Vulnerabilities in the 2017 Breach, Based on Equifax Information



Source: GAO, based on information provided by Equifax. | GAO-18-559

Equifax – problems that helped attackers (1)

- organizational structure: CSO reporting to CLO (Chief Legal Officer)
 - usually CSO/CISO reports to CIO or even to CEO
 - lack of coordination and cooperation
- formal patch management process in place
 - theory: critical patch applied within 48 hours
 - reality: not patched till attack discovery
 - roles in the patch management process not assigned

Equifax – problems that helped attackers (2)

- Equifax was aware of (audit 2015):
 - vulnerabilities were not remediated in a timely manner
 - inadequate asset management procedures (comprehensive IT inventory did not exist)
 - logs retained only for 14/30 days
 - no network segmentation between application servers and the rest of the network
- complex IT environment with poorly documented and operated legacy systems
- expired certificate in network traffic inspection device
 - inspection not functional
 - certificate expired 10 months before the breach
 - 300 expired certificates overall

Case study 2 – Cisco (2022)

- Cisco observed a potential compromise in May 2022 [3]
- Step 1. Attacker gained access:
 - employee personal Google account (not published how)
 - credentials stored in the browser synchronized
 - MFA (push request): voice phishing and MFA fatigue
 - VPN access: new MFA devices (access without victim's cooperation)
- Step 2. Attacker operates inside:
 - escalation to administrative privileges
 - login to multiple systems (this alerted the Cisco Security Incident Response Team)
 - compromising Citrix servers
 - obtained privileged access to domain controllers
 - variety of tools: remote access (LogMeIn, TeamViewer), offensive tools (Cobalt Strike, PowerSploit, Mimikatz, Impacket), standard Windows tools
 - added own backdoor accounts and persistence mechanisms

Case study 2 – Cisco (2022) cont.

- Step 3.
 - attempts to exfiltrate information
 - continuous attempts to re-establish access (after eviction)
 - targeting poor password hygiene, registering domains
 - email communication to executive members
 - files posted on dark web (September 2022)
- Attacker was probably IAB (Initial Access Broker)
 - ties to threat actors UNC2447 (ransomware attacks) and Lapsus\$ (data extortion)
- TTP (Tactics, Techniques, and Procedures) consistent with pre-ransomware activity
- Cisco: a company-wide password reset, and other measures
- no other impact to any products or services, sensitive customer data or sensitive employee information, intellectual property, or supply chain operations, according to Cisco

Case study 3 – Microsoft (2023)

- Microsoft detected an attack on January 2024 [4]
- Midnight Blizzard (NOBELIUM) – a Russia-based threat actor
- initial access:
 - password spray attack (MFA was not enabled)
 - evasion techniques: limited number of accounts, low number of attempts, distributed residential proxy infrastructure
 - compromised a legacy non-production test tenant account
- inside
 - create, modify, grant access to OAuth applications
 - obtaining elevated access to the Microsoft corporate environment
 - finally, granting Office 365 Exchange Online *full_access_as_app* role
 - access to mailboxes (“*including members of our senior leadership team*”)

1. Create a free TryHackMe account (tryhackme.com)
 - verify you can connect via OpenVPN (room OpenVPN)
2. External pentest
 - <https://crz.gov.sk/zmluva/8582224/> (read Appendix 2)
 - pentest specification: the good and the bad (your opinion)
3. Bug bounty programs
 - <https://hackerone.com/visa?type=team>
 - read policy, rules, scope, and out of scope details
 - discuss strengths and problems with this approach to security testing

1. U.S. Government Accountability Office, *Data Protection: Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach*, 2018
2. U.S. House of Representatives, Committee on Oversight and Government Reform, *The Equifax Data Breach*, 2018
3. Nick Biasini, *Cisco Talos shares insights related to recent cyber attack on Cisco*, 2022. <https://blog.talosintelligence.com/recent-cyber-attack/>
4. Microsoft Threat Intelligence: *Midnight Blizzard: Guidance for responders on nation-state attack*, 2024.
<https://www.microsoft.com/en-us/security/blog/2024/01/25/>