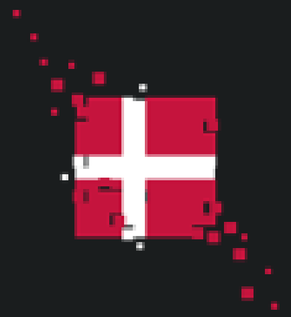
DE DANSKE CYBERMESTERSKABER

Pentesting

An Introduction

Shreyas Srinivasa, Ph.D.
PostDoc Researcher, AAU Copenhagen

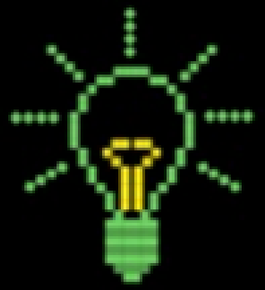
March 02.24



DE DANSKE CYBERMESTERSKABER

DDC 2024

ONLINE
TRÆNINGSDAGE



FEBRUAR-MARTS

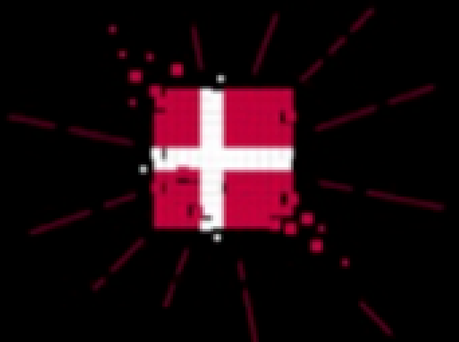
ONLINE
KVALIFIKATION

24.FEB.-17.MARTS

REGIONALE
MESTERSKABER

13. APRIL

DE DANSKE
CYBERMESTERSKABER



4.MAJ

Online træninger (februar – marts)

Online træninger er for ALLE.

Beginner Track

Exploitation Track

Crypto Track

Pentest Track

DE DANSKE
CYBERMESTERSKABER

Online kvalifikation (24. feb. – 17. marts)

Alle kan være med til online kvalifikation, men kun 15-25 årige kan gå videre efterfølgende.

JUNIOR (15-20 ÅR)

(din alder per 31.12.2024)

ONLINE KVALIFIKATION

*KVAL SLUTTER D. 17. MARTS

ÅBNER D. 24. FEBRUAR

SENIOR (21-25 ÅR)

(din alder per 31.12.2024)

ONLINE KVALIFIKATION

*KVAL SLUTTER D. 17. MARTS

ÅBNER D. 24. FEBRUAR

OPEN

Åben for alle, der ikke hører til aldersgruppen 15-25 - Du deltager IKKE i konkurrencen i denne kategori

*KVAL SLUTTER D. 17. MARTS

ÅBNER D. 24. FEBRUAR

DE DANSKE
CYBERMESTERSKABER

DE DANSKE CYBERMESTERSKABER

Pentesting

An Introduction

Shreyas Srinivasa, Ph.D.
PostDoc Researcher, AAU Copenhagen

March 02.24

Agenda

this evening ...

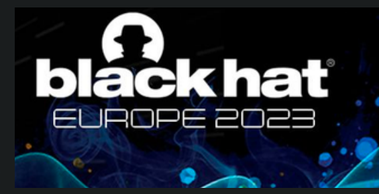
01 Introduction

- Pentesting, vs. Hacking, vs. Red Teaming
- Types
- Workflow

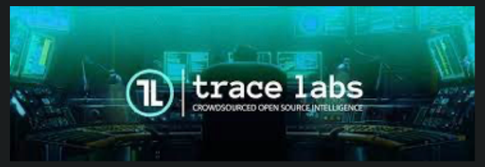
02 Tools & Techniques

- Recon & Enumeration (with NMap, Wappalyzer, Nikto)
- Exploitation (ExploitDB, Metasploit, BurpSuite)
- Reporting

Shreyas Srinivasa,Ph.D.



- 34 yrs, from **Bengaluru**, **India** 🇮🇳
- **Ph.D.** from **Aalborg University**
- Bachelors @ **VTU, India** and Masters @ **TU Darmstadt, Germany**
- Work: 2 yrs in NOC, 6 yrs in SOC
- Research interests: Cyber Threat Intelligence, Cyber Deception, Cyber crime , Internet Security Measurements, OSINT (GOSI)
- Visiting scholar @ **University of Cambridge**, Cambridge Cybercrime Center
- Community service: community worker @**TraceLabs** (finding leads on missing children using OSINT), **Cyberpeace** Institute (NGO)
- Mentor @ **Google Summer of Code** from 2020
- A humble **coffee farmer**



Web: https://sastry17.github.io

Timeline

Introduction

Pentesting

Break - 20 minutes

Elaborate on what you want to discuss.

Techniques and Tools + Activity

Overview of tools and techniques

Haaukins Challenges

Playground

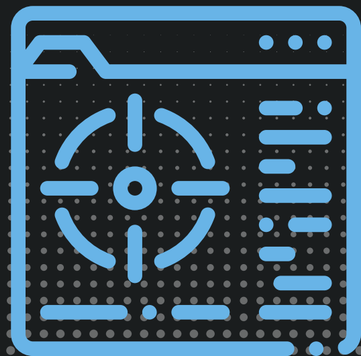
Disclaimer

- This training is an introduction to pentesting and not redteaming
- The training is based on the principle of “Ethical Hacking”
- The aim is to understand preliminary concepts, techniques and tools
- **Please take consent before testing a real target (from the direct owner)**
- Have a legal binding before you perform PenTests
- It is illegal to do Pentests without consent, and can be a punishable offense

Material for today

https://github.com/sastry17/DDC-Pentest/training.zip

PenTesting



Pentesting

What is it?

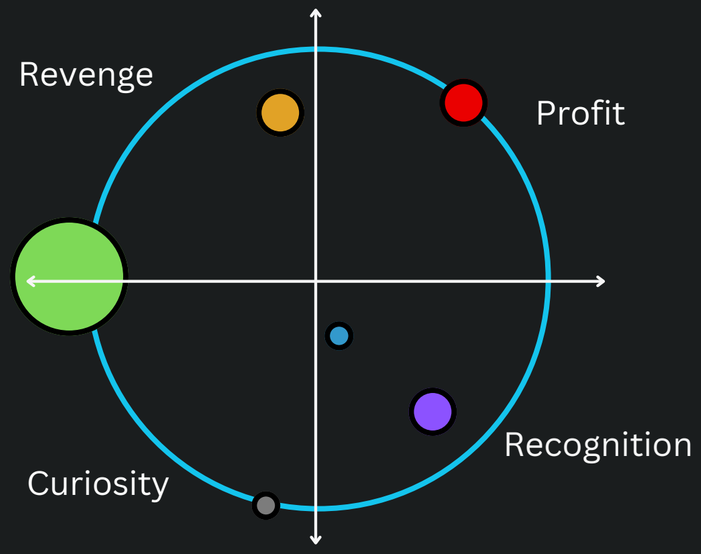
“An ethically agreed, planned and consented process, to test the security of a target system/service from an attacker perspective”

- Goals:
  - Identify the attack surface
  - Improve the security posture
  - Determine and reduce risk
  - Compliance

Pentesting vs Hacking

What it is not?

- Hacking in general perspective is an “Unethical process”
- Hacking does not take consent, and hence there is always a “victim”
- Hacking leads to “Irresponsible Disclosure”, “Loss” or “Harm”
- Hacking is motivated by revenge, monetary profit, haktivism



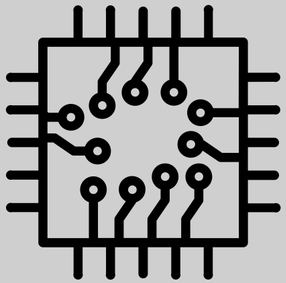
PenTesting vs Red-Teaming

A line of distinction

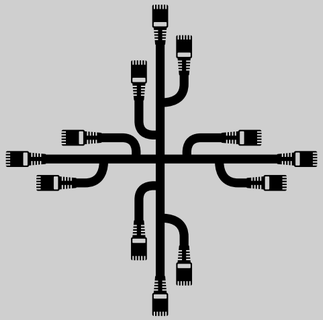
Aspect	PenTesting	Red-Teaming
Objective	Identify and exploit vulnerabilities with an agreed scope	Simulation of real-world attacks to test detection and response capabilities
Scope	Predefined targets and vulnerabilities within a limited timeframe.	Broader scope with multi-stage attacks and several attack vectors
Methodology	Systematic approach and structured process and techniques	Holistic approach that may involve technical attacks, social engineering and physical security assessments
Engagement	Conducted with consent with the target owner, organization/team is fully aware of system under test	Conducted as a secretive process, with the defensive team unaware of the process and timeline

PenTest-Types

Physical access test



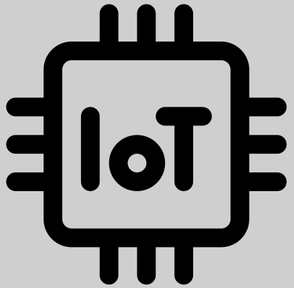
Hardware



Network

Web

App



IoT

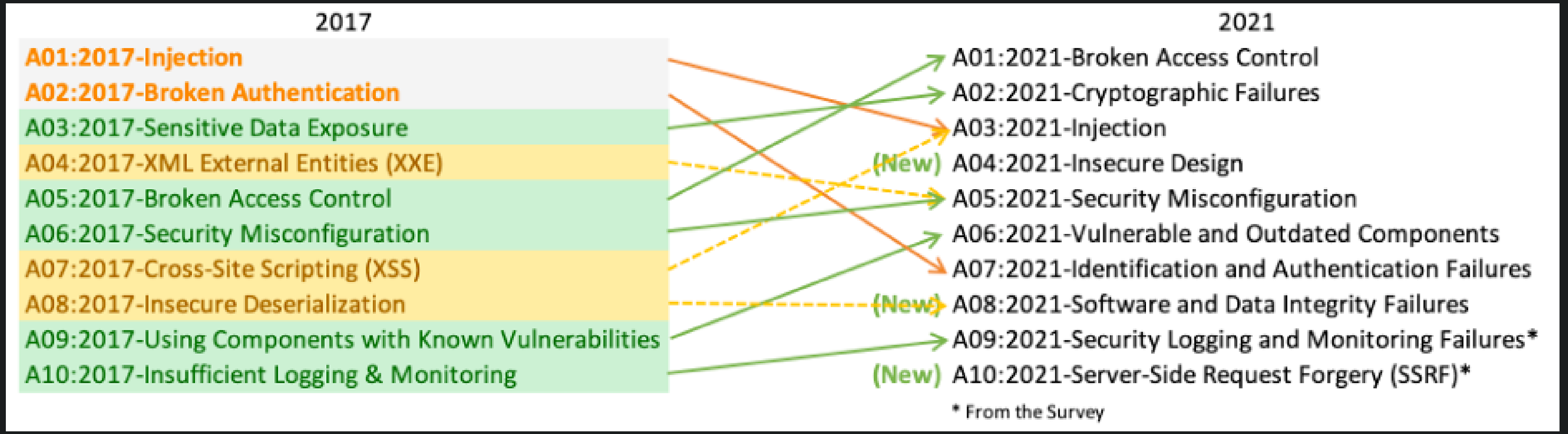
PenTesting Workflow

PenTesting Workflow

src: https://docs.rapid7.com/metasploit/

OWASP top 10 checks

- The OWASP Top 10 is a standard awareness document for developers and web application security.
- It represents a broad consensus about the most critical security risks to web applications



src: https://owasp.org/www-project-top-ten/

OWASP Resources for Web Testing

OWASP Web Penetration Testing Checklist (**19 Pages**)

https://owasp.org/www-project-web-security-testing-guide/assets/archive/OWASP_Web_Application_Penetration_Checklist_v1_1.pdf

OWASP Web Security Testing Guide (**465 Pages**)

https://github.com/OWASP/wstg/releases/download/v4.2/wstg-v4.2.pdf

Break? - (15min)

Tools & Techniques

Recon & Enumeration

- **Recon** - It is the “Information Gathering process”
  - Organizational Intelligence (OPSEC)
  - Metadata collection (DNS records, MX records, Social Engineering, Employee Listing, traceroutes, patents)
- **Enumeration** - Gather information about the target
  - network topology, service discovery, port-scanning
  - web-application enumeration - server software and versions, virtual hosts, folders and paths

Recon & Enumeration - Tools

- Shodan and Censys - OPSec and Information gathering - open ports, services, “history”
- **ExploitDB/searchsploit, NVD** - Database of reported vulnerabilities(NVD) and exploits(ExploitDB)
- **whois, RIPEdb, mxtools** - domain and IP information gathering
- **NMap** - IP Enumeration, Port-scanning, Service Discovery, OS Fingerprinting
- **Wappalyzer** - website technologies JS, CSS, HTML. Works as a browser extension
- **Wfuzz, Recon-ng** - DNS enumeration
- **wafw00f** - WAF detection
- **dirbuster** - web paths and directories

Hands On - Recon

1

- **Shodan & Censys**
  - Open web browser, Go to shodan.io
  - Search for “Telnet”
  - Open another tab on the browser
  - Go to search.censys.com
  - Search for “cybermesterskaberne.dk” :)

2

- **ExploitDB**
  - Open web browser, Go to exploit-db.com
  - Search for “samba” :)

HandsOn- NMap

NMap Activity:

- Launch NMap tool from your machines (Terminal -> nmap)
- type> **nmap scanme.nmap.org**
- Next, type> **nmap -sV scanme.nmap.org**
- Next, type> **nmap -v -O scanme.nmap.org**


```
┌──(sastry17㉿hs24)-[~]
└─$ nmap scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-29 06:43 EST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.18s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 991 closed tcp ports (conn-refused)
PORT      STATE    SERVICE
19/tcp    filtered chargen
22/tcp    open     ssh
53/tcp    open     domain
80/tcp    open     http
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
9929/tcp  open     nping-echo
31337/tcp open     Elite

Nmap done: 1 IP address (1 host up) scanned in 14.15 seconds
```

Activity.1 - 20 mins

Open file “Activity1.pdf” from the zip file.

Exploitation

Exploitation

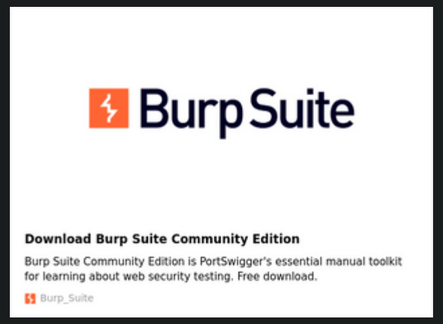
- **Exploitation** - Using the knowledge of vulnerabilities and systems to exploit them for gaining access
- The exploit is determined based on the vulnerabilities identified in the information gathering phase
- However, the exploit needs to be developed or customized (if already developed) and tested
- After exploitation: Gaining control of the system, Privilege Escalation, Pivoting and Gathering evidence
- Techniques - reverse shells, injection attacks
- Tools - **Metasploit Framework(MSF)**, Burp Suite, Zed Applocation Proxy

Exploitation - Metasploit Framework

- MSF Framework : one of the most widely used tools for Pentesting
- Modules - Exploits, Payloads, Auxilliaries, Encoders
- Contains a collection of searchable exploits on diverse types of vulnerabilities
- Components - msfconsole, msfdb, msfvenom, meterpreter

Exploitation - Burp Suite

- comprehensive web application security testing tool that includes a range of features for vulnerability scanning, manual testing, and exploitation
- offers a built-in web proxy, scanner, intruder, repeater, sequencer
- widely used by security professionals and penetration testers for assessing the security posture of web applications.



Activity.2 - 30 mins

Open file “Activity2.pdf” from the zip file.

+ 15 mins break!

Reporting

Reporting

- Generating a report on the findings of the pentest
- Intended for both Management and Technical teams. However, a brief “Management Summary” is included on the overall assessment
- The report includes - how the issue was found, how it was exploited and the remedies

Sample Reporting Structure

Based on: https://owasp.org/www-project-web-security-testing-guide/v42/5-Reporting/README

1. Introduction
    - 1.1 Version Control
    - 1.2 Contents
    - 1.3 The Team
    - 1.4 Scope
    - 1.5 Limitations
    - 1.6 Timeline
    - 1.7 Disclaimer
2. Executive Summary
3. Introduction
    - **3.1 Findings Summary**
    - 3.2 Findings Details
    - 3.3 Remediation
4. Appendices

Ref. ID	Title	Risk Level
1	User Authentication Bypass	High

Questions?

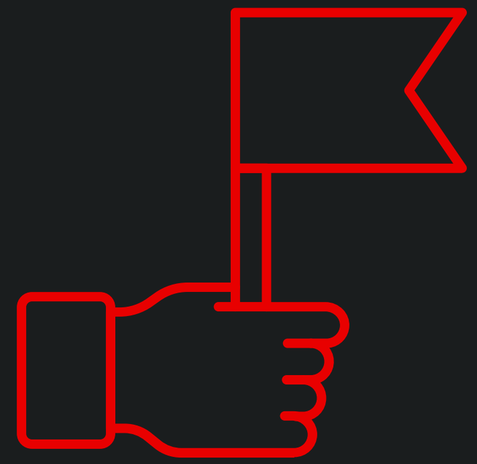
Resources

- **OWASP**
- **The HackTricks Book**
- **PayloadsAllTheThings**
- **Portswigger Academy** ♥
- **HackTheBox Academy**

For the rest of the evening ...

Solve the other challenges at:

https://ddcpentest.cbs.haaukins.com/



DE DANSKE

CYBERMESTERSKABER

PENETRATION TESTING
EVALUATION QR CODE

2. marts 2024

Contact

Shreyas Srinivasa
shreyas.srinivasa@proton.me

Web: https://sastry17.github.io

Thats all Folks