ITS
Institut Teknologi Sepuluh Nopember

ITSEC™
SECURITY DELIVERED

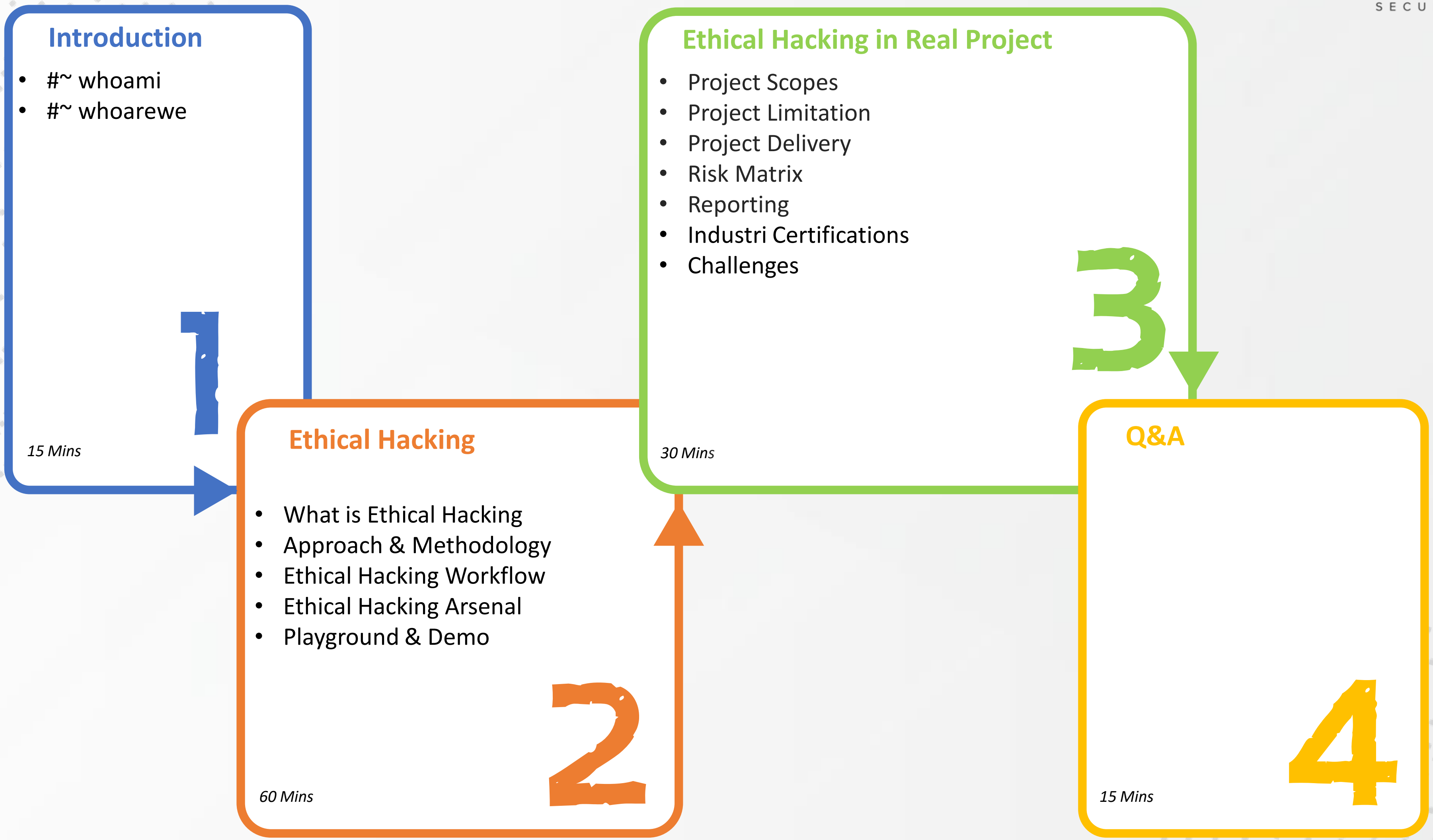
Seminar

Ethical Hacking in Real Project

Link Materi

https://s.id/K1WXj

Agenda



Introduction

- #~ whoami
- #~ whoarewe

1

15 Mins

Ethical Hacking

- What is Ethical Hacking
- Approach & Methodology
- Ethical Hacking Workflow
- Ethical Hacking Arsenal
- Playground & Demo

2

60 Mins

Ethical Hacking in Real Project

- Project Scopes
- Project Limitation
- Project Delivery
- Risk Matrix
- Reporting
- Industri Certifications
- Challenges

3

30 Mins

Q&A

4

15 Mins

Duration : 2 Hours

- Section 01 -

Introduction

Who Am I?

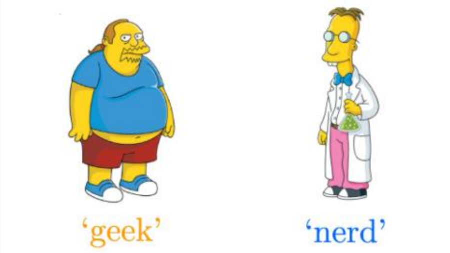
Rio Asepta, M.Kom

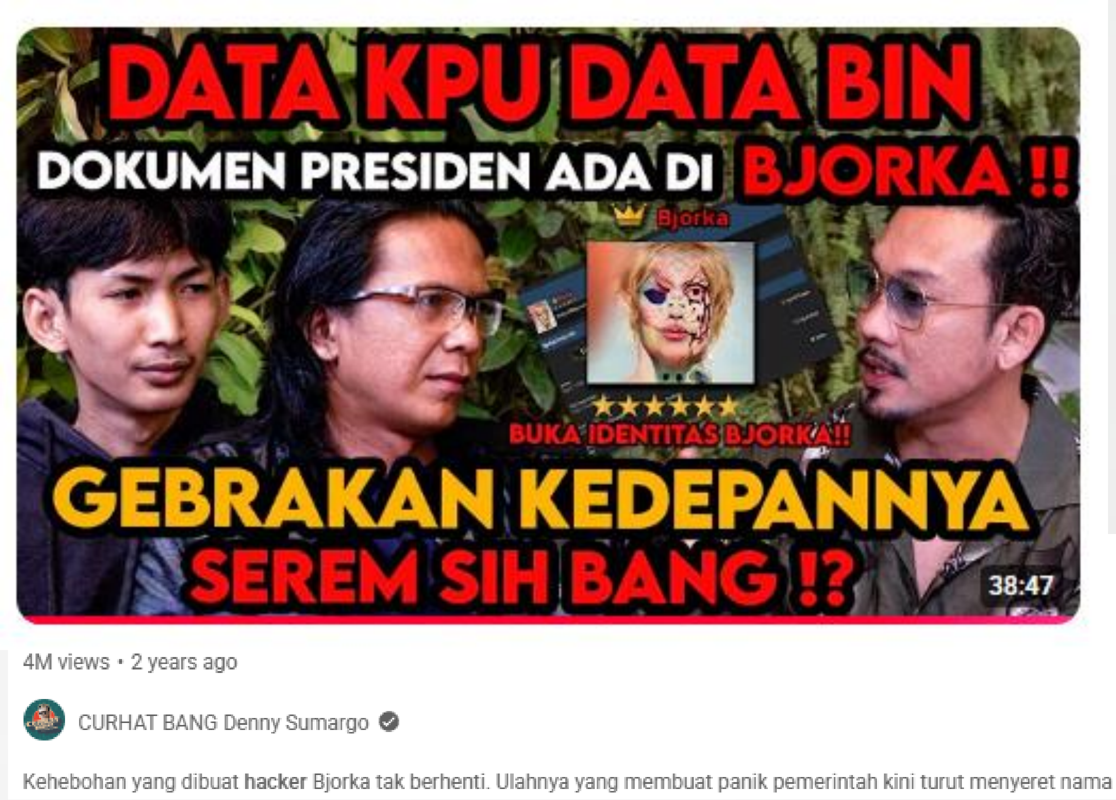
OSCE, OSCP, OSWP, CRTE, CRTP, CEH, ECSA

- **Principal Consultant – ITSEC Asia**
  Almost 10 years of experience with more than 500 penetration testing & Red Teaming project deliveries.

- **Trainer & Speaker**
  BSSN, Polri (Cyber Crimes), TNI, governments and private companies.

- **Parrot & AirsoftGun & Keris Lover**
  So, I am Not Geek! ~~I am a Nerd!~~





4M views • 2 years ago

CURHAT BANG Denny Sumargo

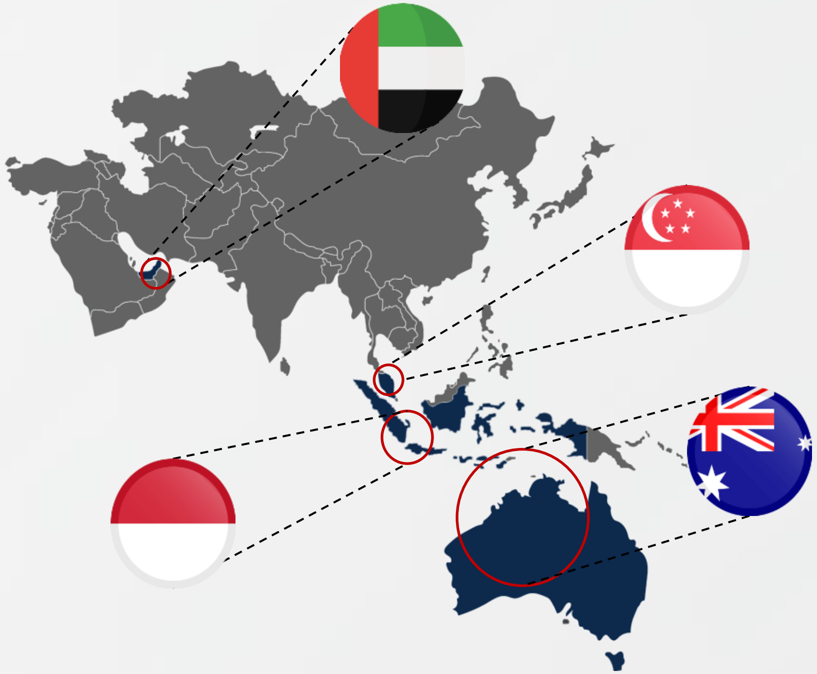
Kehebohan yang dibuat **hacker** Bjorka tak berhenti. Ulahnya yang membuat panik pemerintah kini turut menyeret nama

ITSEC
SECURITY DELIVERED

Who Are We?

ITSEC is a leading APAC cybersecurity company, listed on the Indonesian stock exchange (IDX), with over 270 employees in five countries. We deliver end-to-end cybersecurity services and solutions, including Consulting Services, Security Solutions Integration and Managed Security Services. ITSEC provides continuous IT infrastructure protection against multiplying cybersecurity threats, and compliance with increasingly demanding data protection and critical infrastructure regulations.

Our expertise has been built from over a decade of delivering thousands of high-quality cybersecurity projects, providing cutting-edge solutions in collaboration with world-class technology partners across financial, telecommunication, energy, transportation, manufacturing and other critical industry sectors. We also have extensive experience helping our customers with fraud prevention, operational technology (OT) and Industrial IoT (IIoT) security.



CYBR

2023
Listed on the IDX
(Indonesian Stock Exchange)

15 Years
Of Experience

100+
Active Clients

5,000+
Projects

270+
Professional Personnel

Offices
Indonesia, Singapore, Australia, Dubai

Accredited & Certified

ITSEC Asia is a member of CREST and holds ISO 27001, ISO 9001 and ISO 14001 certifications

Consultant : **OSCE3, OSCE, OSEP, OSWE, OSED, OSCP, OSCE, CRT, CPSA, CRTE, CRTP, CISSP, CISA, CISM, CSXF, CSXP, CEH, GPEN, GSEC, GCIA, GCIH, GDPR, ISA/IEC62443**

Project Management : **PMP, P2P, P2AP, ITIL-F, CSM, CSPO, CITPM, ICP-ACC**

SWIFT CSP Assessment and Cyber Security Service Providers

Our ISO 9001, ISO 27001, ISO 14001 logos pertain to services delivered by PT ITSEC Asia

Our Services

Penetration Testing & Red Teaming

Audit, Risk Assurance & Compliance

Security Solution Integration

Managed Security Services

OT/IoT Security

Information Security Analysis

Application Security

Threat Hunting (Compromise Assessment)

Digital Forensic & Incident Response

V-CISO

Our Managed Solutions

Fraud Management

Delivered **the largest Fraud Management System** in South East Asia

DevSecOps

Delivered **DevSecOps for the largest bank** in South East Asia

SOC

Delivered **SOC for the largest bank** in South East Asia

- Section 02 -

Ethical Hacking

Ethical Hacking

ITSEC
SECURITY DELIVERED

Introduction

Ethical Hacking or Penetration Testing is authorized permission and approval to evaluate the vulnerability in cyber security of a computer system or network by simulating an attack from malicious source **(e.g. malicious hackers)**

Objectives

- **Determine** presence of vulnerabilities **in the information system (applications, infrastructure, people and processes)**
- **Practically evaluate quality of implemented security measures**
- **Determine capabilities in detecting and reacting to cyber attacks**
- **Increase security awareness**

Methodology

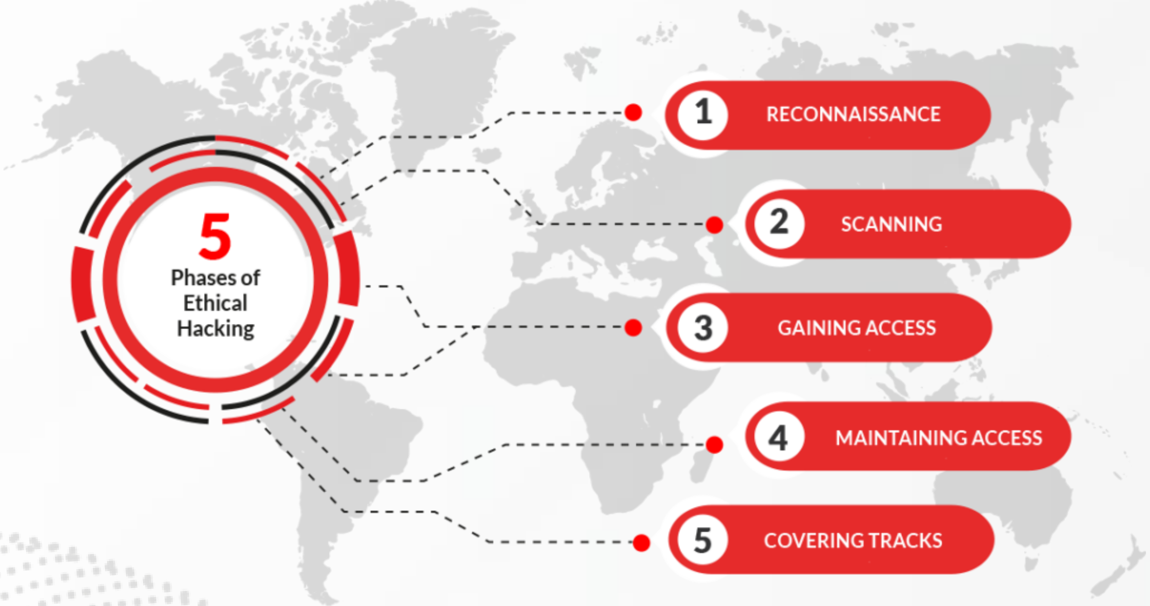
Methodology basics

- Securing CIA
  - Confidentiality, Integrity, Availability of Information Assets
- Common standards:
  - Open Source Security Testing Methodology Manual (OSSTMM), For General Pentest
  - Information Systems Security Assessment Framework (ISSAF), For VA & Infra/Network
  - OWASP Testing Guide Chapter 4; For Web & API
  - OWASP Mobile Security Testing Guide ; For IOS & Android

Source:

- OSSTMM: https://www.isecom.org
- ISSAF: https://oissg.org
- OWASP: https://owasp.org

Approach



- **1. Reconnaissance**
  Reconnaissance refers to the preparatory phase where an attacker seeks to gather information about a target prior to launching an attack.

- **2. Scanning**
  Scanning utilizes different tools to collect information on websites, networks, or file systems to detect vulnerabilities.

- **3. Gaining Access**
  Gaining Access is where an attacker gets access to a system or application that is on a network or computer.

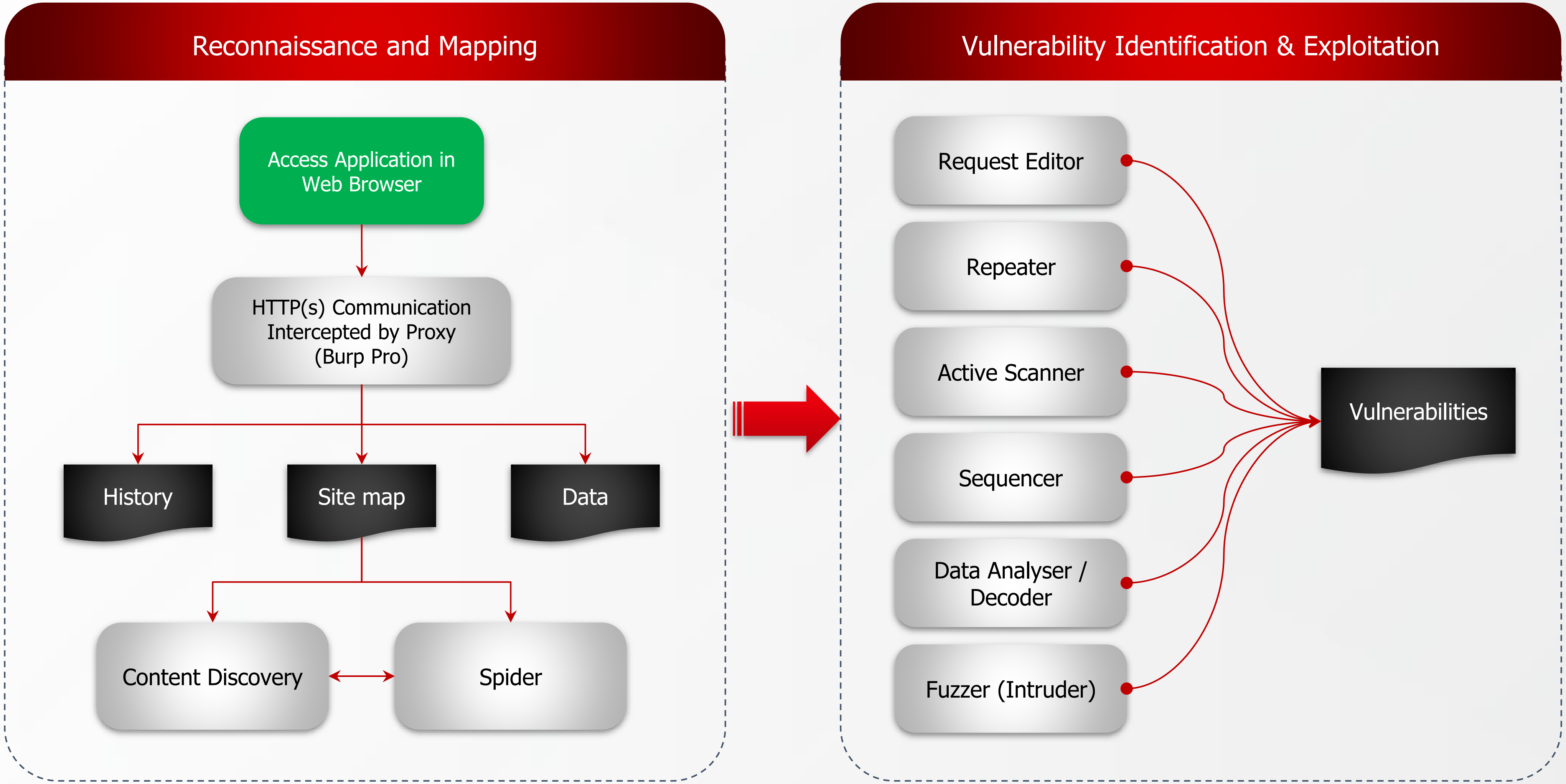
- **4. Maintaining Access**
  Maintaining Access also referred to as persistence. This allows an attacker continued access on a target whether the machine is rebooted, or the user is logged off.

- **5. Covering Tracks**
  Covering Tracks After gaining access to a target, removing any artifacts is critical to ensure you as an attacker does not leave a trace. This may include deleting logs, removing any tools, scripts, or applications that were installed on the target.

Source:

- https://www.eccouncil.org/cybersecurity-exchange/ethical-hacking/ceh-learning-framework/

Workflow – Web Apps


Reconnaissance and Mapping
Access Application in Web Browser
HTTP(s) Communication Intercepted by Proxy (Burp Pro)
History
Site map
Data
Content Discovery
Spider
Vulnerability Identification & Exploitation
Request Editor
Repeater
Active Scanner
Sequencer
Data Analyser / Decoder
Fuzzer (Intruder)
Vulnerabilities

OWASP TOP 10 2021

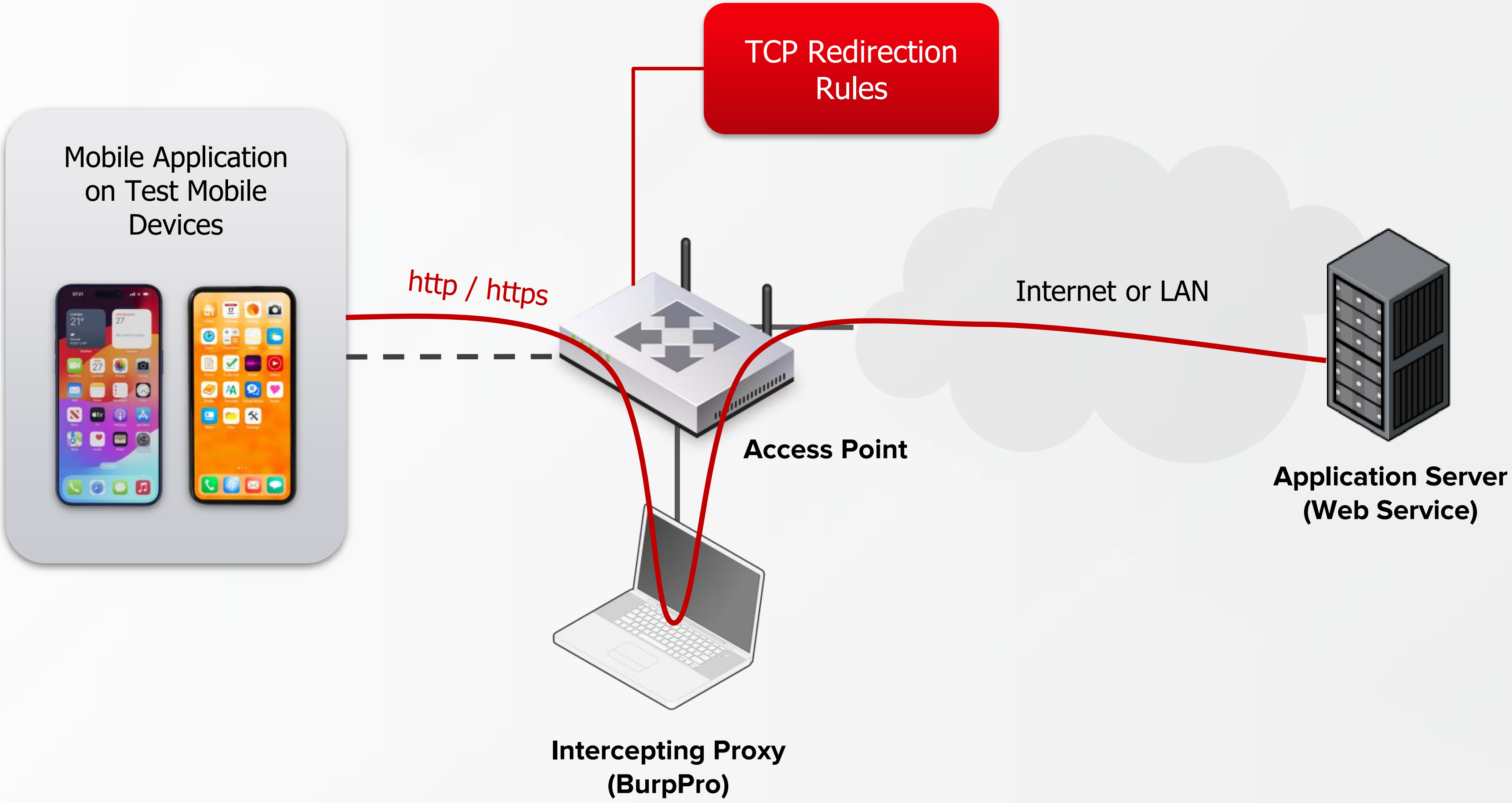
Top 10 Web Application Security Risks (2021)

A1	Broken Access Control
A2	Cryptographic Failures
A3	Injection
A4	Insecure Design
A5	Security Misconfiguration
A6	Vulnerable and Outdated Components
A7	Identification and Authentication Failures
A8	Software and Data Integrity Failures
A9	Security Logging and Monitoring Failures
A10	Server Side Request Forgery (SSRF)

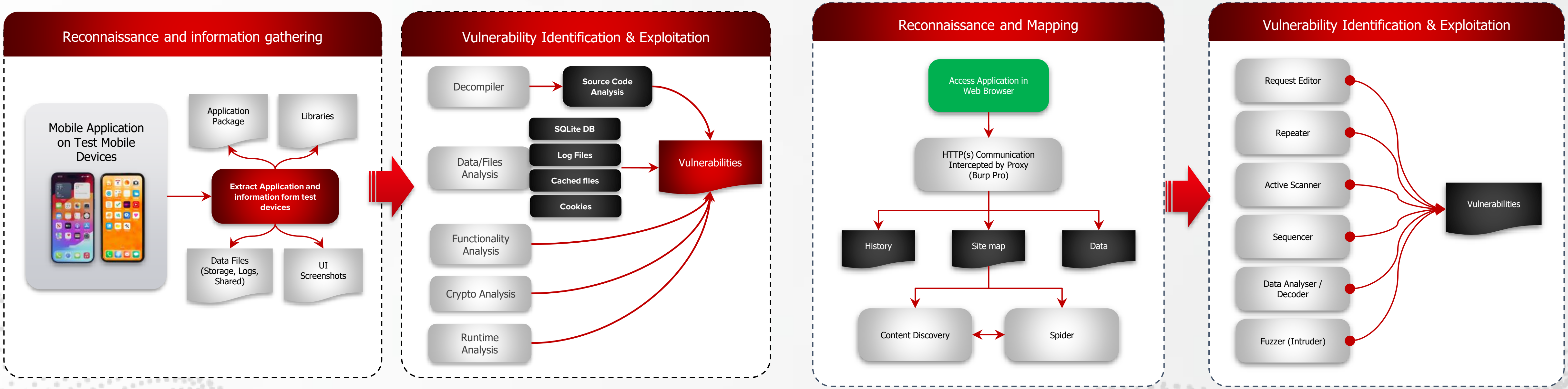
Source:

- https://owasp.org/Top10/

Workflow – Mobile Apps


TCP Redirection Rules
Mobile Application on Test Mobile Devices
http / https
Internet or LAN
Access Point
Application Server (Web Service)
Intercepting Proxy (BurpPro)

Workflow – Mobile Apps



Reconnaissance and information gathering

Mobile Application on Test Mobile Devices

Extract Application and information form test devices

Application Package

Libraries

Data Files (Storage, Logs, Shared)

UI Screenshots

Vulnerability Identification & Exploitation

Decompiler

Source Code Analysis

Data/Files Analysis

SQLite DB

Log Files

Cached files

Cookies

Functionality Analysis

Crypto Analysis

Runtime Analysis

Vulnerabilities

Reconnaissance and Mapping

Access Application in Web Browser

HTTP(s) Communication Intercepted by Proxy (Burp Pro)

History

Site map

Data

Content Discovery

Spider

Vulnerability Identification & Exploitation

Request Editor

Repeater

Active Scanner

Sequencer

Data Analyser / Decoder

Fuzzer (Intruder)

Vulnerabilities

OWASP TOP 10 Mobile 2024

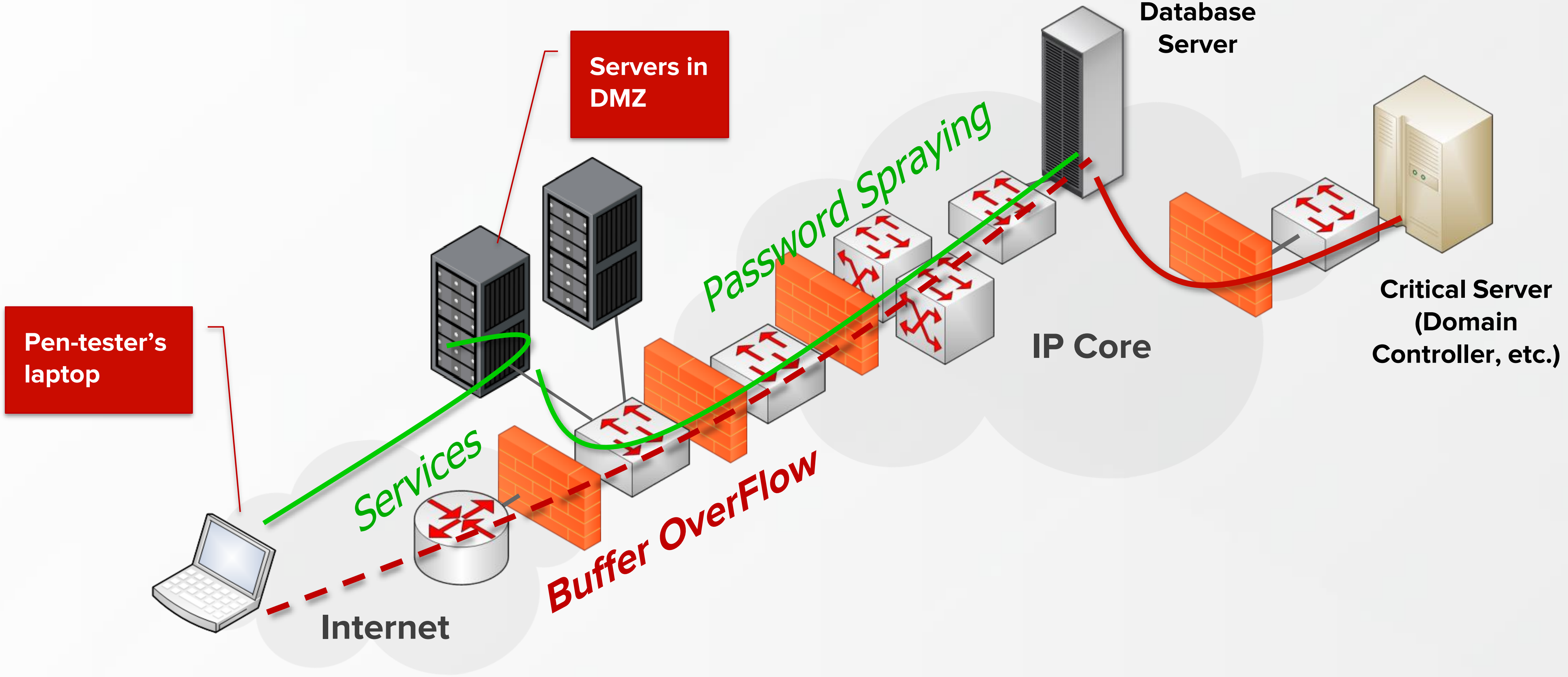
Top 10 Mobile Risks (2024)

- **M1** Improper Credential Usage
- **M2** Inadequate Supply Chain Security
- **M3** Insecure Authentication/ Authorization
- **M4** Insufficient Input/Output Validation
- **M5** Insecure Communication
- **M6** Inadequate Privacy Controls
- **M7** Insufficient Binary Protections
- **M8** Security Misconfiguration
- **M9** Insecure Data Storage
- **M10** Insufficient Cryptography

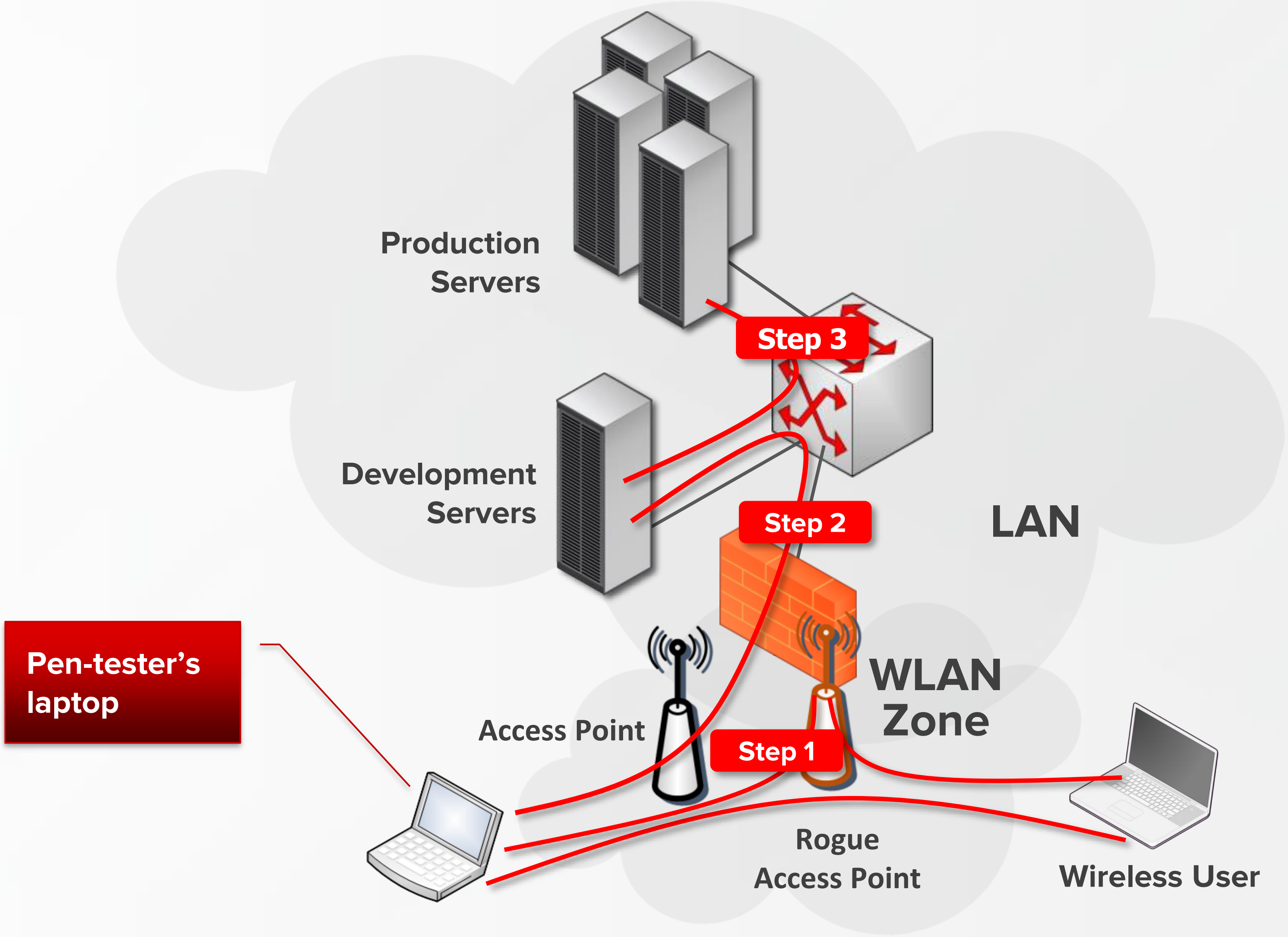
Source:

- https://owasp.org/www-project-mobile-top-10/

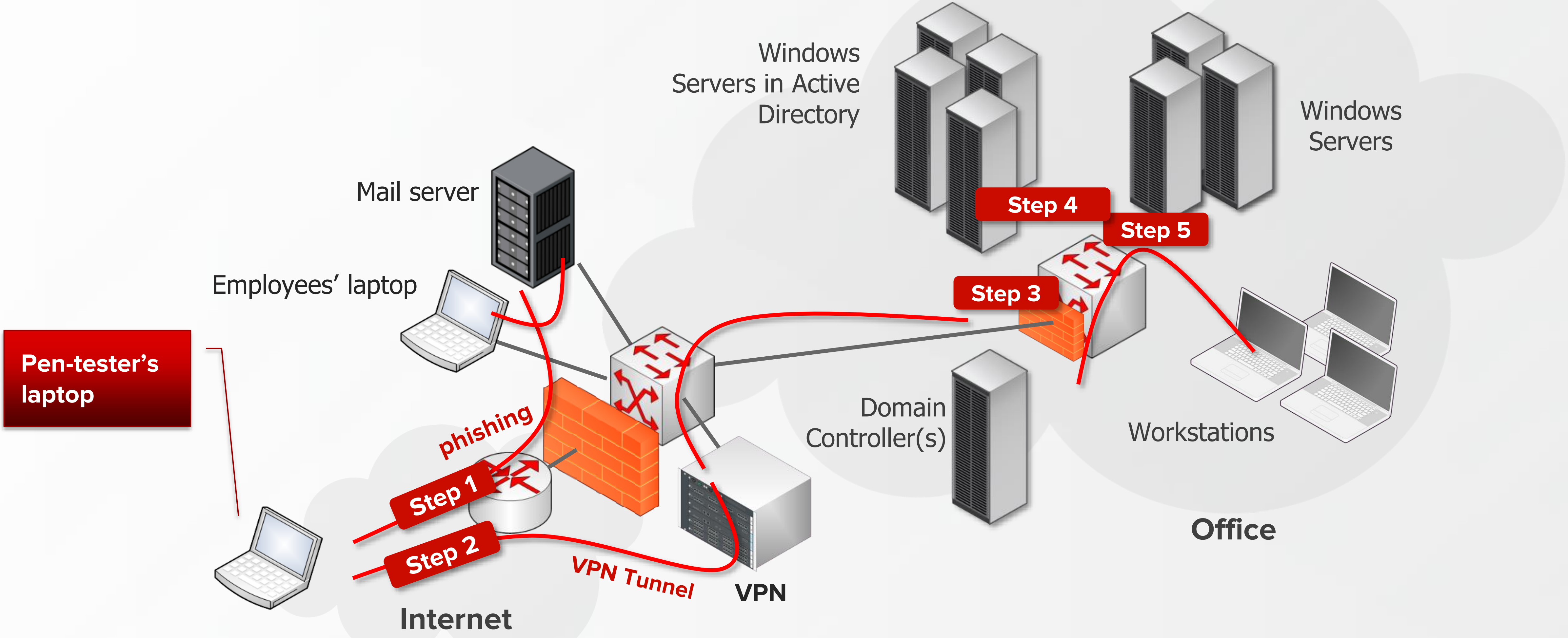
Workflow – Infrastructure



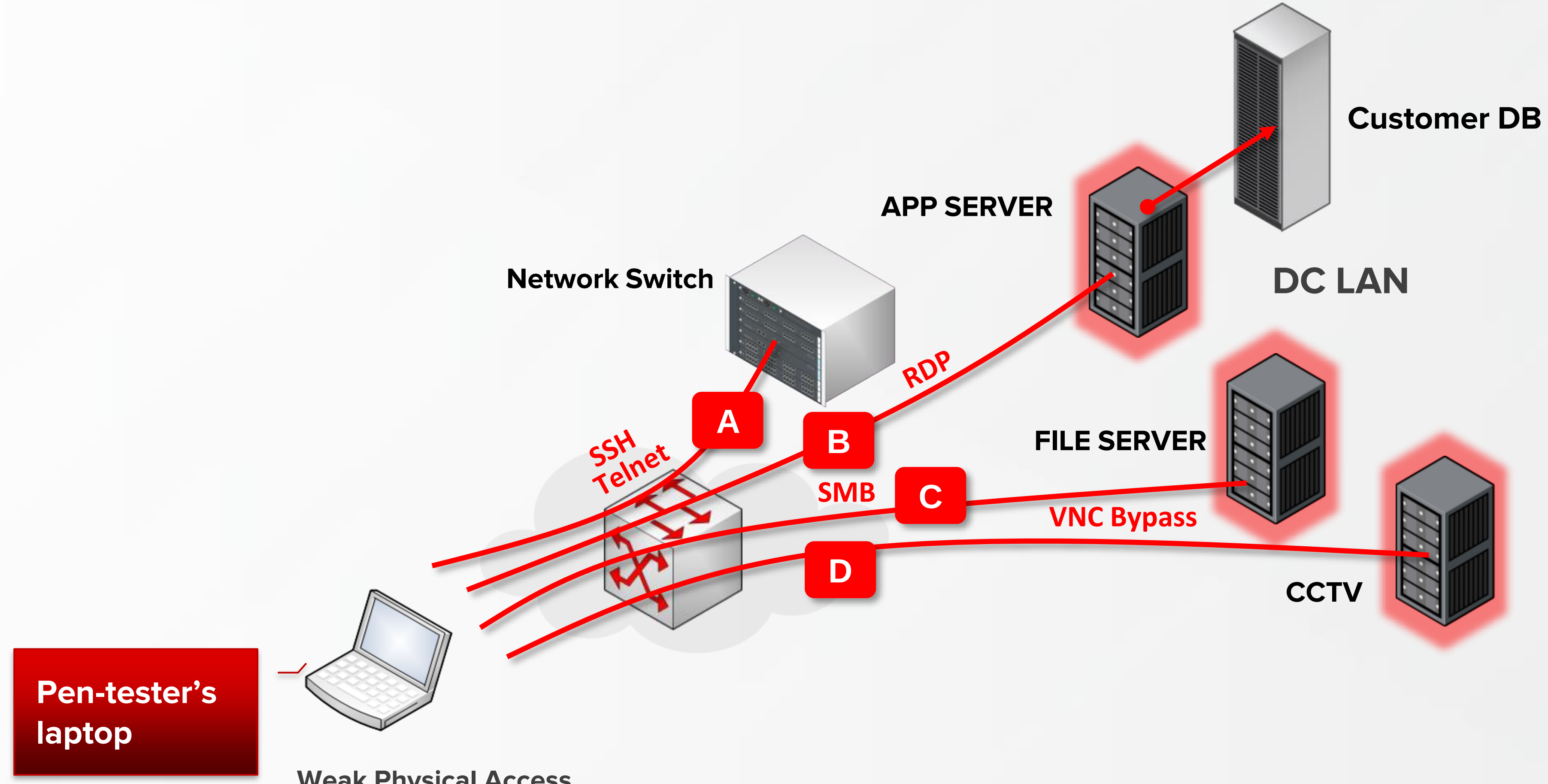
Workflow – Wireless



Workflow – Social Engineering



Workflow – Physical



Weak Physical Access Protection (Office LAN, ATM, etc.)

Penetration Testing Arsenals

Mindset

- Curiosity
- Creativity
- Persistence & Dedication
- Logical and analytical thinking skill
- Think outside the box
- Adaptability and willing to learn new things

Penetration Testing Arsenals

Operating System (OS)

- Kali Linux
- Parrot OS
- BlackArch
- BackBox
- Etc.

Applications

- Nmap
- Metasploit Framework
- Nessus
- Nikto
- Nuclei
- Hydra
- CrackMapExec
- Impacket Libraries
- Hashcat
- SQLMap
- Burp Suite
- Wireshark
- Custom Tools from Github Repository
- Personal Proprietary

Playground

Hack The Box

Lab: Web application, Infrastructure penetration test
Source: https://www.hackthebox.com/

Vuln Hub

Lab: Web application, Infrastructure penetration test
Source: https://www.vulnhub.com/

Metasploitable

Lab: Infrastructure (Linux) penetration test
Source: https://www.metasploit.com/

DVWA

Lab: Web application penetration test
Source: https://github.com/digininja/DVWA

Demo

- Section 03 -

Ethical Hacking in Real Project

Penetration Testing Principles

Do's

- Maintain proper documentation:
  - Take screenshot with timestamp of every significant action
  - Record who/what/when
- Be able to explain details on how vulnerability was identified & exploited
- Ensure secure communications of results:
  - Distribution of findings on need to know basis (also within pen-test team)
- Encrypt all data and communications
- Follow relevant standards and procedures
- Do everything possible to minimize risks

Don'ts

- No significant actions on production system
- No unauthorized major changes to the system, application and network
- No tests not agreed with client
- Never store or e-mail confidential data unencrypted

Scopes of Penetration Testing

Web Application

Mobile Application
- **Android**
- **iOS**

IT Infrastructure
- **Server, Database, Router, Switch, Firewall, Antivirus, etc.**
- **Wireless**

Thick Client
- **Desktop Application**

Cloud
- **AWS, Google Cloud, Azure, etc**

SWIFT Banking

Rest API

Physical Building
- **DC & DRC**
- **Head Quarter & Office Building**

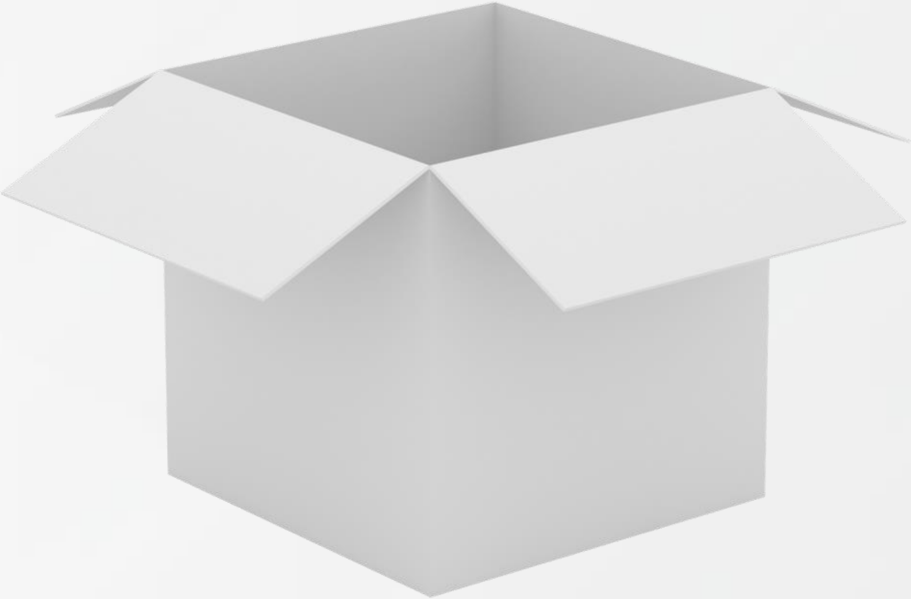
Social Engineering
- **Email Phishing**
- **Social Media Phishing**

EDC & ATM
- **Conventional EDC**
- **Smart EDC**
- **ATM Machine**

Internet of Things (IoT)
- **Smart Devices**

Approaches

Black box



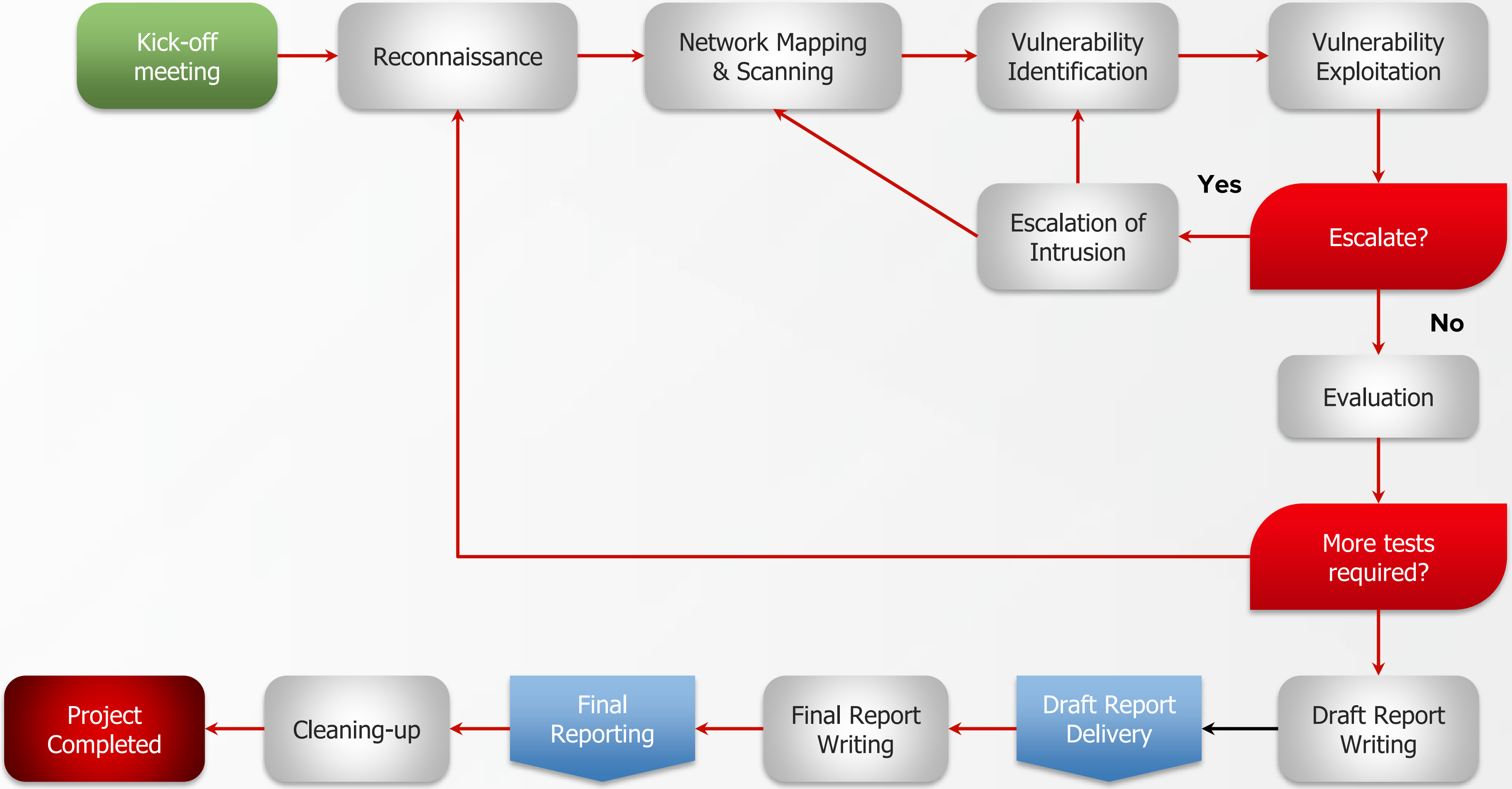
White box

29

Approaches

External and Internal

Penetration Testing Process



Risk Matrix Calculation:

Risk ratings provided in this report are estimated using the following matrix:

LIKELIHOOD

Almost Certain	MEDIUM	HIGH	HIGH	EXTREME	EXTREME
Likely	MEDIUM	MEDIUM	HIGH	EXTREME	EXTREME
Possible	LOW	MEDIUM	MEDIUM	HIGH	EXTREME
Unlikely	LOW	LOW	MEDIUM	HIGH	HIGH
Rare	LOW	LOW	LOW	MEDIUM	HIGH
	Insignificant	Minor	Moderate	Major	Catastrophic

CONSEQUENCE
(IMPACT)

Definitions:

- ***Likelihood***
  A rough measure of how likely this particular vulnerability is uncovered and exploited by an attacker.
- ***Impact***
  An estimate of the magnitude of the effect on the system (confidentially, integrity, and availability) if the vulnerability were exploited.

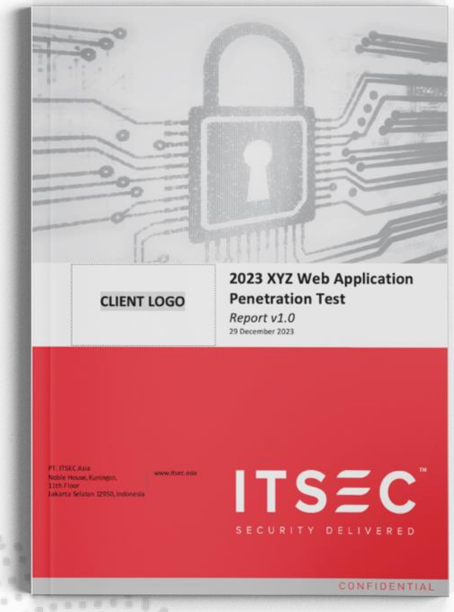
Report Structure

Final Report

- Overview
- Executive Summary
- Finding Title, Risk & Status
- Finding Description
- Threat & Risk
- Recommendation
  - Corrective Action
  - Preventive Action
- Finding PIC
- Based Standard & Policies
- Reference
- Remediation Result

The final report will be sent after remediation test completed

Sample Report of Penetration Test



CLIENT LOGO

2023 XYZ Web Application Penetration Test

Report v1.0

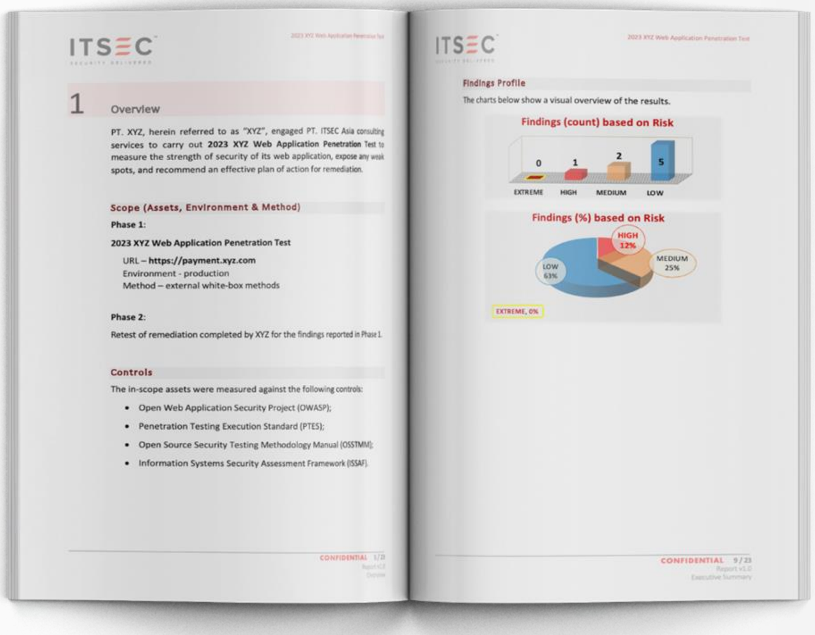
29 December 2023

PT. ITSEC Asia
Noble House, Kuningan,
11th Floor
Jakarta Selatan 12950, Indonesia

www.itsec.asia

ITSEC
SECURITY DELIVERED

CONFIDENTIAL



2023 XYZ Web Application Penetration Test

1 Overview

PT. XYZ, herein referred to as "XYZ", engaged PT. ITSEC Asia consulting services to carry out **2023 XYZ Web Application Penetration** Test to measure the strength of security of its web application, expose any weak spots, and recommend an effective plan of action for remediation.

Scope (Assets, Environment & Method)

Phase 1:

2023 XYZ Web Application Penetration Test

URL – **https://payment.xyz.com**
Environment - production
Method – external white-box methods

Phase 2:

Retest of remediation completed by XYZ for the findings reported in Phase 1.

Controls

The in-scope assets were measured against the following controls:

- Open Web Application Security Project (OWASP);
- Penetration Testing Execution Standard (PTES);
- Open Source Security Testing Methodology Manual (OSSTMM);
- Information Systems Security Assessment Framework (ISSAF).

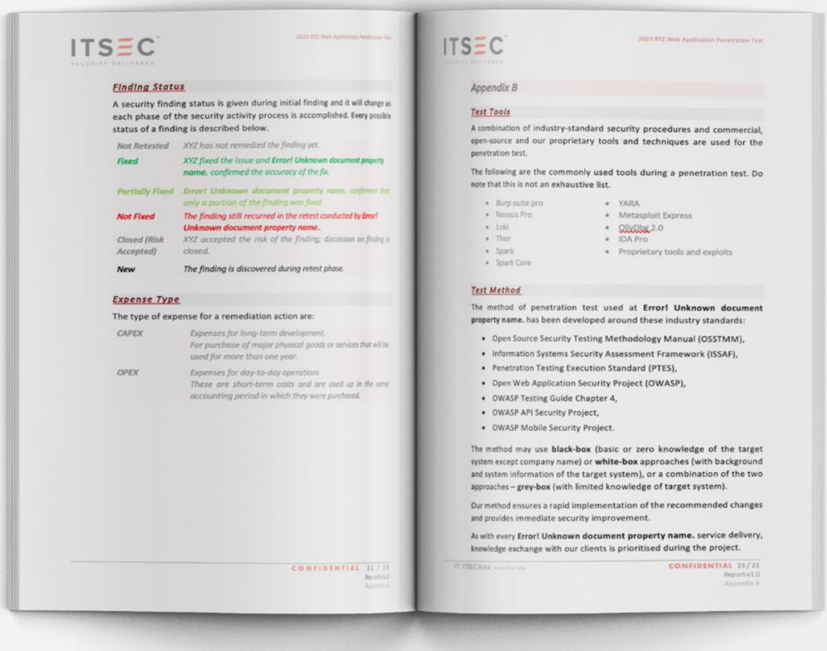
CONFIDENTIAL 1/23
Report v1.0
Overview

2023 XYZ Web Application Penetration Test

Findings Profile

The charts below show a visual overview of the results.

CONFIDENTIAL 9/23
Report v1.0
Executive Summary



2023 XYZ Web Application Penetration Test

Finding Status

A security finding status is given during initial finding and it will change as each phase of the security activity process is accomplished. Every possible status of a finding is described below.

Not Retested	*XYZ has not remedied the finding yet.*
Fixed	*XYZ fixed the issue and **Error! Unknown document property name.** confirmed the accuracy of the fix.*
Partially Fixed	*Error! Unknown document property name. confirmed that only a portion of the finding was fixed.*
Not Fixed	*The finding still recurred in the retest conducted by **Error! Unknown document property name.**.*
Closed (Risk Accepted)	*XYZ accepted the risk of the finding; discussion on finding is closed.*
New	*The finding is discovered during retest phase.*

Expense Type

The type of expense for a remediation action are:

CAPEX	*Expenses for long-term development.* *For purchase of major physical goods or services that will be used for more than one year.*
OPEX	*Expenses for day-to-day operations* *These are short-term costs and are used up in the same accounting period in which they were purchased.*

CONFIDENTIAL 22 / 23
Report v1.0
Appendix A

2023 XYZ Web Application Penetration Test

Appendix B

Test Tools

A combination of industry-standard security procedures and commercial, open-source and our proprietary tools and techniques are used for the penetration test.

The following are the commonly used tools during a penetration test. Do note that this is not an exhaustive list.

- Burp suite pro
- Nessus Pro
- Loki
- Thor
- Spark
- Spark Core
- YARA
- Metasploit Express
- OllyDbg 2.0
- IDA Pro
- Proprietary tools and exploits

Test Method

The method of penetration test used at **Error! Unknown document property name.** has been developed around these industry standards:

- Open Source Security Testing Methodology Manual (OSSTMM),
- Information Systems Security Assessment Framework (ISSAF),
- Penetration Testing Execution Standard (PTES),
- Open Web Application Security Project (OWASP),
- OWASP Testing Guide Chapter 4,
- OWASP API Security Project,
- OWASP Mobile Security Project.

The method may use **black-box** (basic or zero knowledge of the target system except company name) or **white-box** approaches (with background and system information of the target system), or a combination of the two approaches – **grey-box** (with limited knowledge of target system).

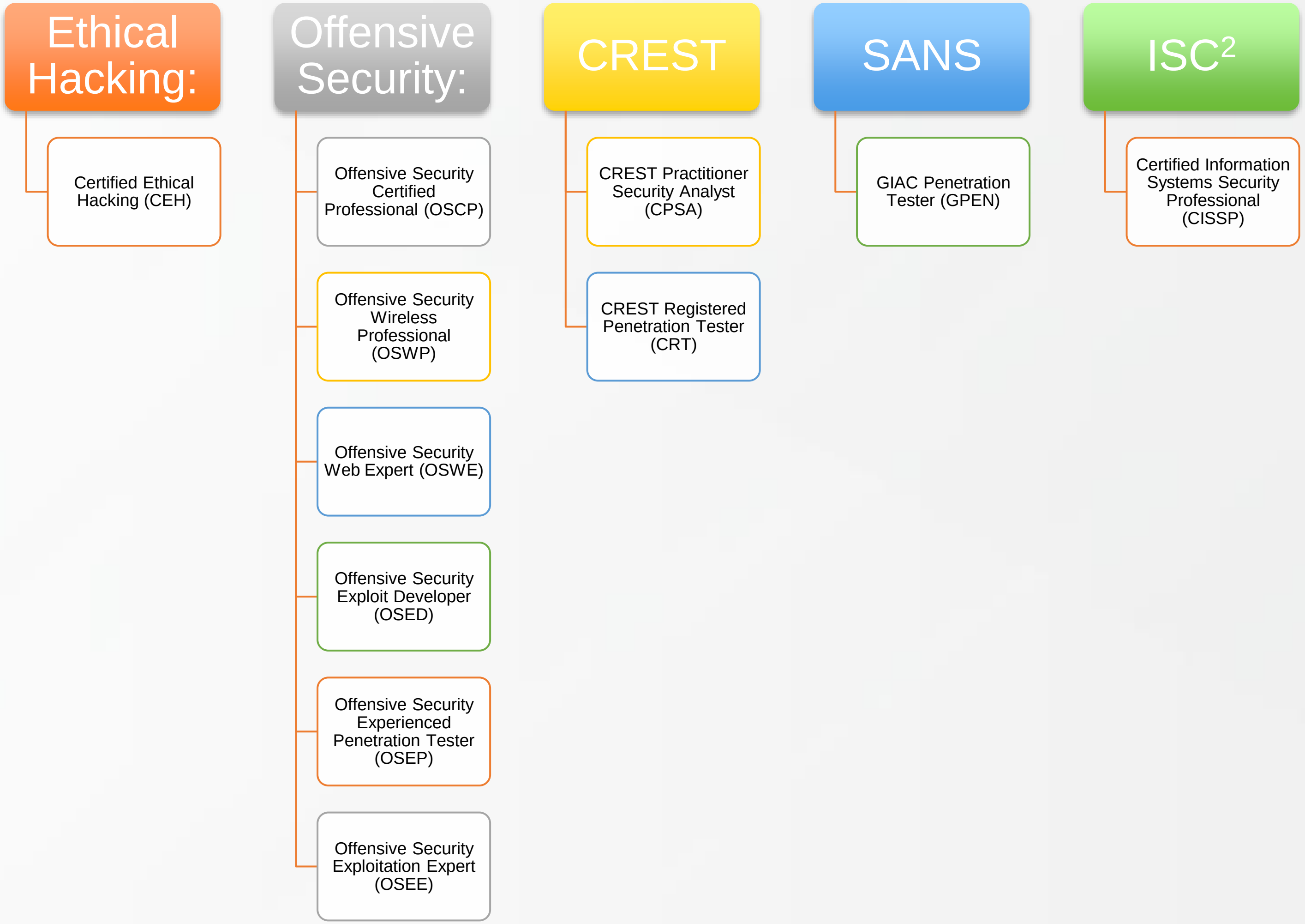
Our method ensures a rapid implementation of the recommended changes and provides immediate security improvement.

As with every **Error! Unknown document property name.** service delivery, knowledge exchange with our clients is prioritised during the project.

PT. ITSEC Asia www.itsec.asia

CONFIDENTIAL 23 / 23
Report v1.0
Appendix B

Industrial Certification



Ethical Hacking:

- Certified Ethical Hacking (CEH)

Offensive Security:

- Offensive Security Certified Professional (OSCP)
- Offensive Security Wireless Professional (OSWP)
- Offensive Security Web Expert (OSWE)
- Offensive Security Exploit Developer (OSED)
- Offensive Security Experienced Penetration Tester (OSEP)
- Offensive Security Exploitation Expert (OSEE)

CREST

- CREST Practitioner Security Analyst (CPSA)
- CREST Registered Penetration Tester (CRT)

SANS

- GIAC Penetration Tester (GPEN)

ISC^2

- Certified Information Systems Security Professional (CISSP)

Challenges - Offensive

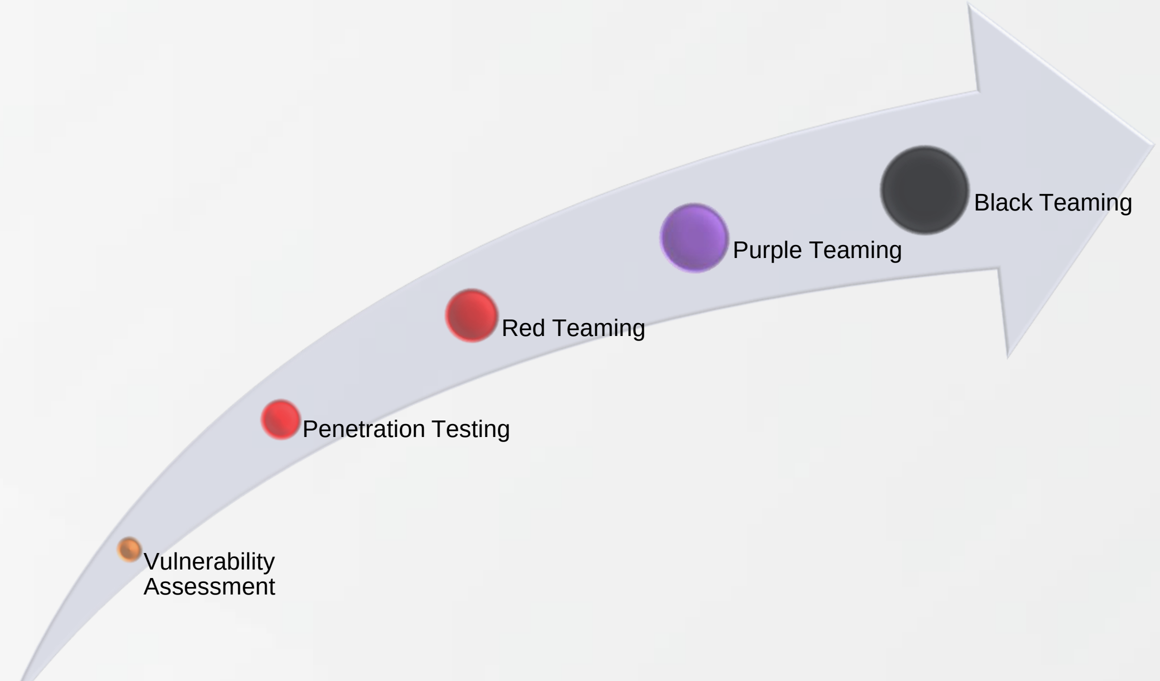
- **Vulnerability Assessment (VA)**
  The process of identifying vulnerabilities without exploitation attempt on the identified vulnerabilities. This includes manual and automated approaches.

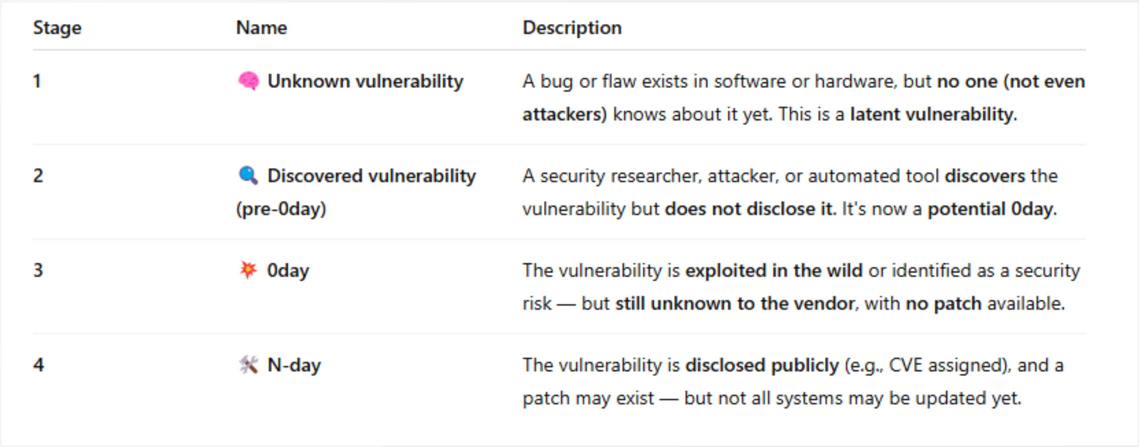
- **Penetration Testing (PenTest)**
  penetration testing goes a step further from VA by attempting to exploit those weaknesses.

- **Red Teaming**
  By using Tactic, Technique & Procedure (TTP) to test how well a mature organization can detect, respond to, and recover from real-world threats.

- **Purple Teaming**
  Cybersecurity exercise collaboration where both the Red Team (offensive) and the Blue Team (defensive) work together to improve an organization’s detection, defense, and response capabilities.

- **Black Teaming**
  -0day attack simulation!





Stage	Name	Description
1	🧠 **Unknown vulnerability**	A bug or flaw exists in software or hardware, but **no one (not even attackers)** knows about it yet. This is a **latent vulnerability.**
2	🔍 **Discovered vulnerability (pre-0day)**	A security researcher, attacker, or automated tool **discovers** the vulnerability but **does not disclose it.** It's now a **potential 0day.**
3	💥 **0day**	The vulnerability is **exploited in the wild** or identified as a security risk — but **still unknown to the vendor**, with **no patch** available.
4	🛠️ **N-day**	The vulnerability is **disclosed publicly** (e.g., CVE assigned), and a patch may exist — but not all systems may be updated yet.

Challenges - Defensive

It costs lot more to defend computer system than it costs to attack it.

- Section 04 -

Q & A

Thank You

INDONESIA
Noble House, Level 11.
Jakarta 12950, Indonesia

contact@itsec.asia
+62 (21) 29783050

SINGAPORE
112 Robinson Road, #11-04
Singapore 068902

contact@itsec.sg
+65 3159 1145

AUSTRALIA
Level 18, 390 St Kilda Road
Melbourne Victoria 3004

info@itsec.com.au
+61 403 185 051