# Vulnerability Assessment
# &
# Peentration Testing
# (VAPT)

KamiLimu - cyber security
cohort 9

# Check in

How are you doing?

# Vulnerability assessment & penetration testing (VAPT's)

These are a general set of exercises undertaken by companies to determine their cyber security posture.

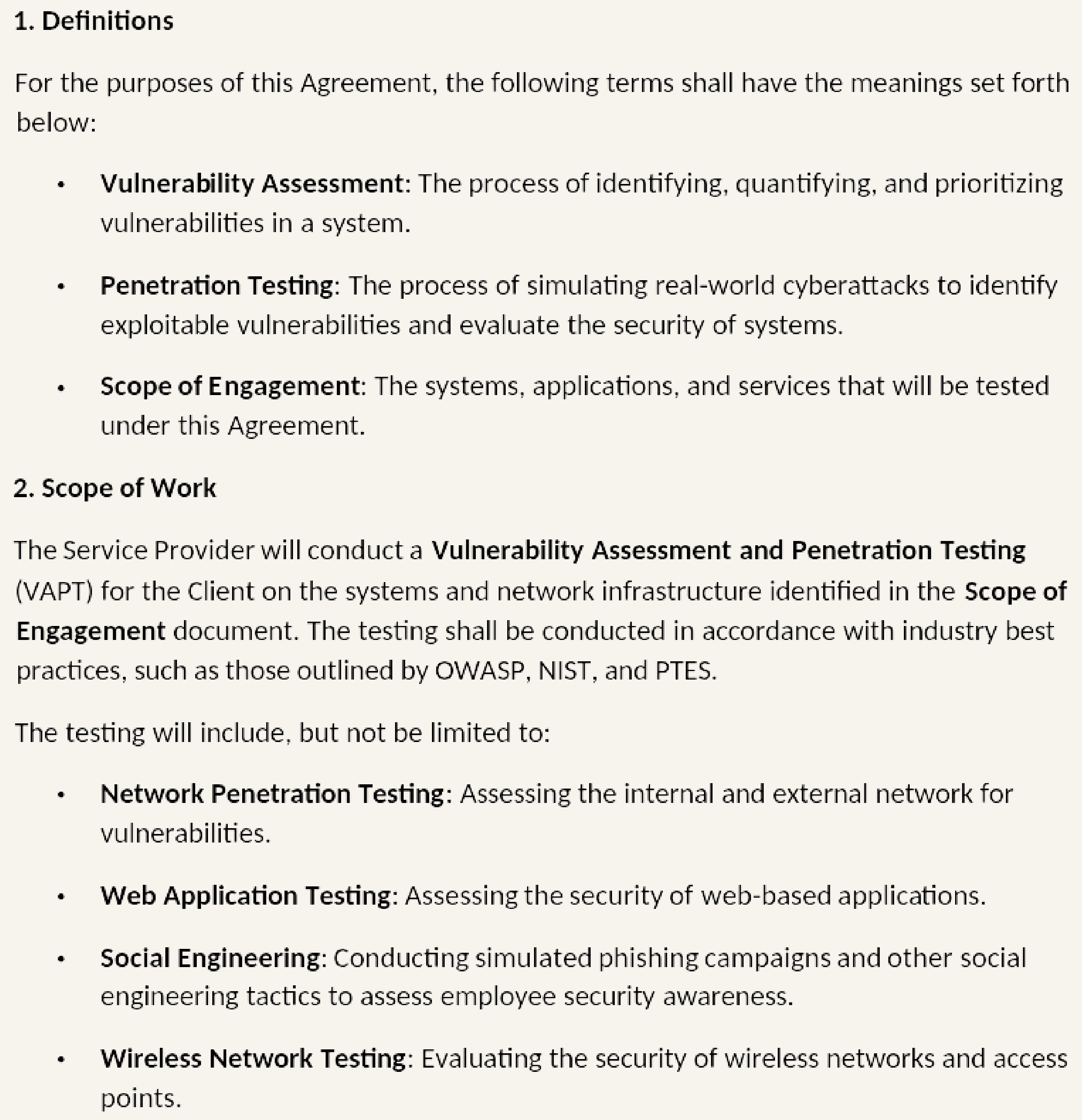
The major steps taken in a VAPT are:

- Scope review + permissions
- Vulnerability assessment
- Penetration Test activities
- Reporting
- Client engagement + presentations

# Permission, permission, permission... (and scope)

# What does permission look like?

- Usually a written document
- Ideally lays out the kind of engagement e.g Penetration Test
- Defines what to assess and what not to assess



**1. Definitions**

For the purposes of this Agreement, the following terms shall have the meanings set forth below:

- **Vulnerability Assessment**: The process of identifying, quantifying, and prioritizing vulnerabilities in a system.
- **Penetration Testing**: The process of simulating real-world cyberattacks to identify exploitable vulnerabilities and evaluate the security of systems.
- **Scope of Engagement**: The systems, applications, and services that will be tested under this Agreement.

**2. Scope of Work**

The Service Provider will conduct a **Vulnerability Assessment and Penetration Testing** (VAPT) for the Client on the systems and network infrastructure identified in the **Scope of Engagement** document. The testing shall be conducted in accordance with industry best practices, such as those outlined by OWASP, NIST, and PTES.

The testing will include, but not be limited to:

- **Network Penetration Testing**: Assessing the internal and external network for vulnerabilities.
- **Web Application Testing**: Assessing the security of web-based applications.
- **Social Engineering**: Conducting simulated phishing campaigns and other social engineering tactics to assess employee security awareness.
- **Wireless Network Testing**: Evaluating the security of wireless networks and access points.

# Vulnerability Assessments

Usually, a simple scan of an environment, system, network or application (or other), to identify where the vulnerabilities are & how severe they are.

Usually done with tooling including...

Nessus N ™
X nexpose ®
NMAP
MOBSF
AN ALL-IN-ONE MOBILE APPLICATION SECURITY ASSESSMENT FRAMEWORK
PORTSWIGGER
WEB SECURITY
Q
QUALYS
ON DEMAND SECURITY
w3af
SCOUTSUITE
MediaWiki
OpenVAS
osvdb

# Vulnerability Assessment output

Usually a (long) list of findings

Can be organised in a spreadsheet, dashboard etc.

Contains the finding, location and severity (low, medium, high, critical)

Shared with the organization with a note to immediately "patch" the findings

# Penetration Test

This is the “exploitation” phase of an engagement where you are supposed to test as many vulnerabilities as you can find.

### Reconnaissance (information gathering)

What can you find about the environment?

### Vulnerability discovery & exploitation

What are the weaknesses in the environment?

### Lateral movement & privilege escalation

How far can you go (or what can you do) with the weaknesses identified?

Culminates in a report showing what you exploited, how and how to fix (remediate) the bug

# Other engagements...

Sometimes, you may be faced with these unique aspects to "VAPT's" that don't always fit the standard mold...

- Application reviews
- Red Team assessments
- Network architecture reviews
- G.R.C reviews
- Social Engineering (stand-alone)
- ... more

# Reporting

# Reporting

The most valuable/important part of the entire assessment

Communicates what you found and how to fix it

Helps senior management know where their risks are

Allows IT to fix their weaknesses before the “bad” guys find them

Really valuable skill to have so learn to write and communicate findings clearly.

Take notes during the engagement so you don’t forget anything!

# Good to know - resources

Be familiar with the following tools/resources...

- G.R.C assessment frameworks including:
  - ISO 27001
  - ITGCs
  - NIST
  - COBIT

- CVSS scoring system (3.0/3.1/4.0) - Valuable for understanding severity ratings of vulnerabilities.

- Mitre Att&ck Framework - red teaming guidance

- cisa.gov known vulnerabilities & exploits (kve) - great for exploits to known vulnerabilities

- Note-taking & screenshot tools:
  - Obsidian
  - Cherry Tree
  - Greenshot
  - more...

# Practical

HTB Academy - Attacking Enterprise Networks (here)

# Thank you!

# Questions?