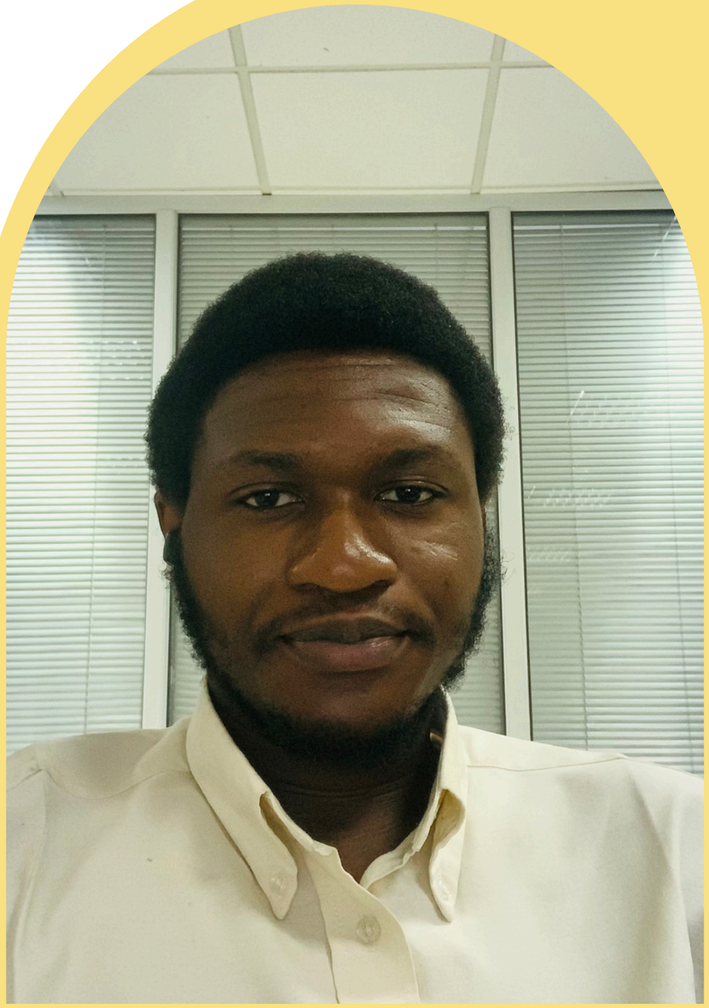
Hacktales

HackTales Red Team Internship

MENTOR: DANIEL JOHNSON



Whoami

Instructor: Daniel Johnson

Info: Hacker, Security Researcher, Red Teamer, AppSec & SecDevOps Engineer, Military Intelligence enthusiast, Anime & Philosophy lover & Avid Gamer.
Certifications: eJPT, HTB CPTS, PNPT (in-view), OSCP (in-view)
Socials: https://www.linkedin.com/in/daninyourcomputer/
Personal site: https://hesrami.github.io

Background
Bsc CyberSecurity, Previously worked in military intelligence, currently work in Telecoms & Fintech Industry with a passion for IT /Offensive Security Instructing and breaking Active Directory.

What is Ethical Hacking?

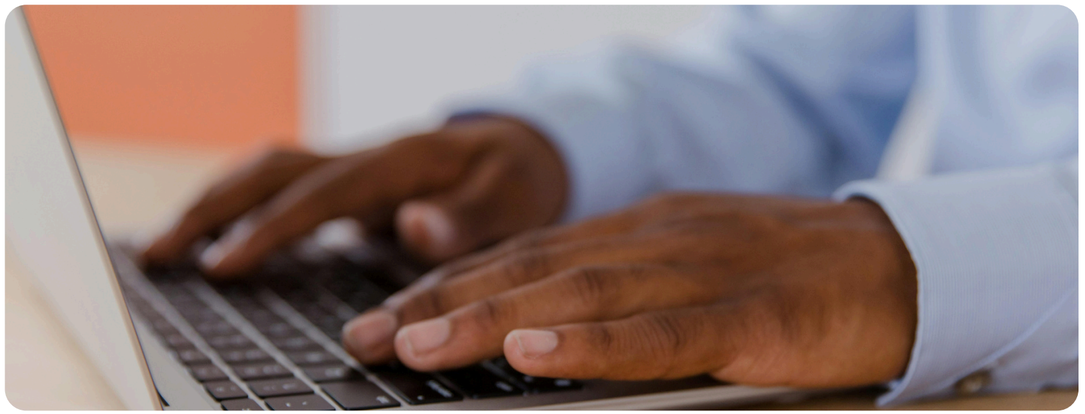
Course Objectives

- Real World Career
- Awareness
- Certificate Preparation

What we will cover: Session I Syllabus

Foundational Topics:

- Ethical Hacking definition, Legalities & Standards
- Phases of a pentest
- Information Gathering/Reconnaissance
- Introduction to virtualization & Lab Setup
- Attacking common network services
- Cryptography & Hashing, breaking cryptographic algos & Hash cracking
- Utilizing Reverse shells to compromise applications Metasploit framework
- Detecting & Exploiting the OWASP top 10 (2021) Linux Privilege Escalation
- Active Directory Fundamentals



PLEASE ONLY USE THE INFORMATION LEARNED IN THIS COURSE FOR ETHICAL PURPOSES ONLY.

PHASES OF A PENETRATION TEST

- Pre - Engagement
- Information Gathering
- Vulnerability Assessment
- Exploitation
- Post Exploitation
- Post Engagement

PRE-ENGAGEMENT

STAGE I

DEFINITION

The step before the real penetration test is called pre-engagement. Numerous inquiries are made, and some contracts are signed, during this phase. After learning about the client's needs, we provide a thorough explanation on how to optimize the test. A scoping questionnaire that defines the scope of assets that are within our access are stated & Contracts are drawn up

SIGNIFICANCE

Clearly defines our limits during a test in form of Rules of Engagement, communicates legally binding conditions between us and the client via Non-Disclosure Agreements which might be involved, and informs the client of possible risks. Documents involved: Rules of engagement, Scoping Document, Scoping Questionnaire, NDA, Contract.

INFORMATION GATHERING

STAGE II

DEFINITION:

This is the phase in which we gather all available information about the company, its employees and infrastructure, and how they are organized. Information gathering is the most frequent and vital phase throughout the penetration testing process, to which we will return again and again. It is also known as Reconnaissance.

TYPES: ACTIVE & PASSIVE RECONNAISSANCE

SIGNIFICANCE

Defines an attack surface for us. Can be divided into

Open-Source Intelligence Infrastructure Enumeration

Service Enumeration Host Enumeration

VULNERABILITY ASSESSMENT

STAGE III

DEFINITION:

During the vulnerability assessment phase, we examine and analyze the information gathered during the information gathering phase. The vulnerability assessment phase is an analytical process based on the findings.

SIGNIFICANCE

Vulnerability identification is typically the outcome.

Utilizing Descriptive analysis, this is the phase where we utilize common vulnerability identifiers and standards to describe what we have found as well as their severity, one of such standard is the CVE(Common Vulnerabilities & Exposure) & CVSS (Common Vulnerability Scoring System) scaling

EXPLOITATION

STAGE IV

DEFINITION:

In the exploitation step, we search for ways to modify these vulnerabilities to fit our use case and gain the desired role (e.g., elevated privileges, a foothold, etc.). The PoC must be changed to run the code in order for the target machine to connect back to us over (preferably) an encrypted connection to an IP address we provide if we wish to obtain a reverse shell. Thus, the planning of an exploit is mostly included in the step of exploiting.

SIGNIFICANCE:

Weaponisation of identified vulnerability from the vulnerability assessment phase is performed here, this phase is crucial in establishing access into the targets network/asset.

POST EXPLOITATION

STAGE V

DEFINITION:

Let's assume we successfully exploited the target system during the Exploitation stage. As with the Exploitation stage, we must again consider whether or not to utilize Evasive Testing in the Post-Exploitation stage. We are already on the system in the post-exploitation phase, making it much more difficult to avoid an alert. The Post-Exploitation stage aims to obtain sensitive and security-relevant information from a local perspective and business-relevant information that, in most cases, requires higher privileges than a standard user

SIGNIFICANCE:

This phase includes:

- Evasive testing
- Pillaging
- Maintaining access (Persistence)
- Data Exfiltration & Lateral Movement
- Information Gathering

POST-ENGAGEMENT

STAGE VI

DEFINITION:

We must perform many activities (many of them contractually binding) after our scans, exploitation, lateral movement, and post-exploitation activities are complete. No two engagements are the same, so these activities may differ slightly but generally must be performed to close out an engagement fully. This phase is characterized by cleanup of scripts and revert of actions performed within the client network as well as reporting & documentation of all findings in clear and concise terms with remediation actions.

SIGNIFICANCE:

The Penetration test document is the one most important document and the only deliverable that shows proof of security issues in the client network which is essentially the purpose of the pentest. It must have an executive summary section in simple non technical terms that provides a high level overview for executive clients to read and understand the business risks the findings pose.

LAWS

NDPA

The Nigerian Data Protection Act is a law that protects the personal data of Nigerian citizens. It was signed into law on June 12, 2023.

It establishes a legal framework for the processing of personal data

- It aims to balance innovation and the protection of privacy rights
- It gives individuals more control over their personal information
- It ensures that businesses and organizations act responsibly when collecting, storing, and processing data

How NPDA affects you as a Pentester?

LEGAL IMPLICATIONS & CONSENT

- Unauthorized penetration testing or ethical hacking without explicit written consent from the organization is illegal under NDPA.
- You must ensure that all testing agreements explicitly state the scope of the test and obtain a signed authorization letter to avoid legal risks.

How NPDA affects you as a Pentester?

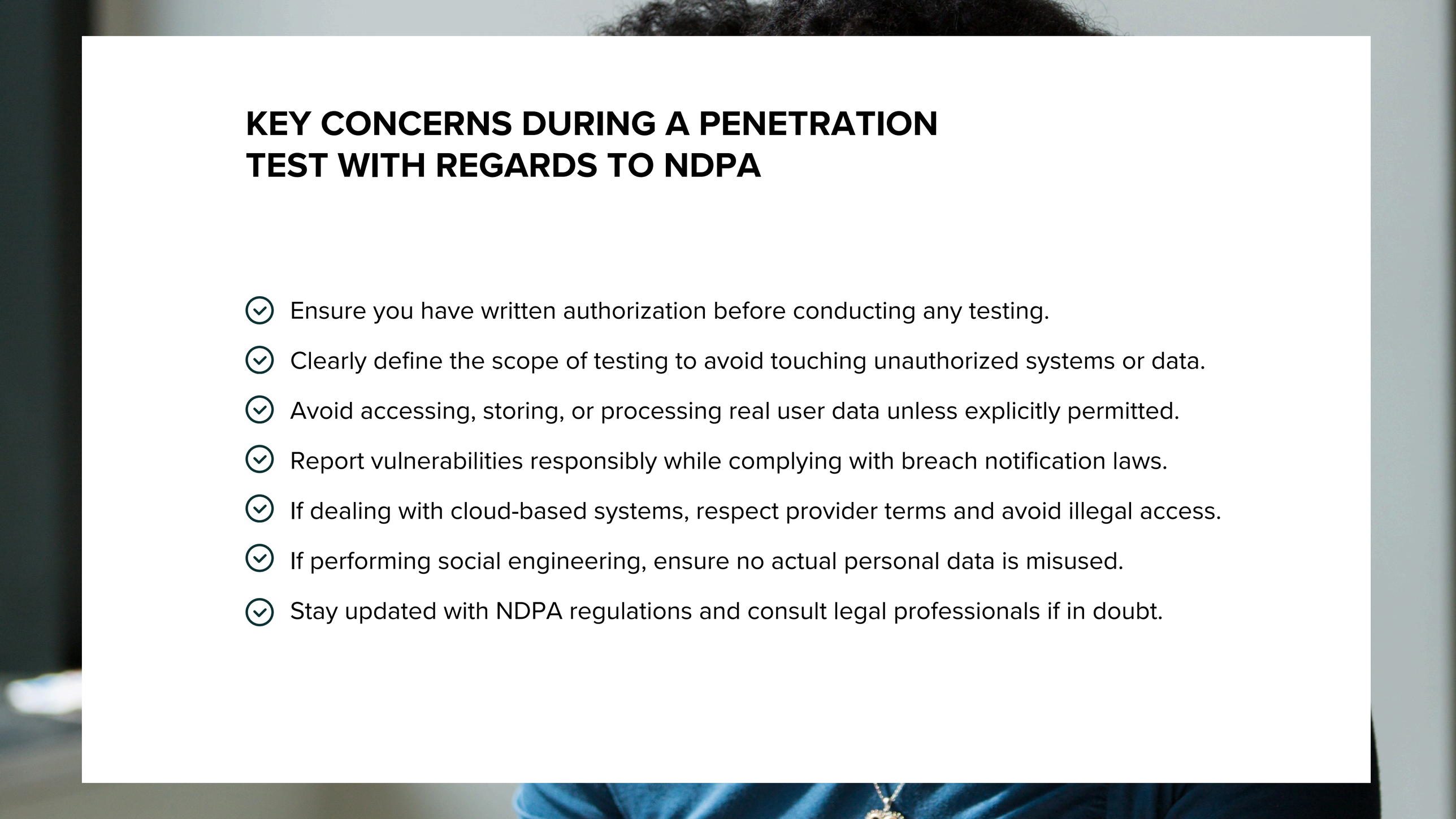
HANDLING PERSONALLY IDENTIFIABLE INFORMATION (PII)

- If your test exposes or accesses PII (e.g., customer data, employee records), you must not store, share, or process it outside the defined scope.
- Secure handling and proper data disposal are critical to avoid legal violations.
- Data Breach Reporting Requirements

How NPDA affects you as a Pentester?

DATA BREACH REPORTING REQUIREMENTS

- If you discover a security vulnerability leading to a data breach, organizations may be legally required to report it within 72 hours to the Nigeria Data Protection Commission (NDPC).
- As a tester, you should document the issue properly and advise the organization on compliance steps.



KEY CONCERNS DURING A PENETRATION TEST WITH REGARDS TO NDPA

- Ensure you have written authorization before conducting any testing.
- Clearly define the scope of testing to avoid touching unauthorized systems or data.
- Avoid accessing, storing, or processing real user data unless explicitly permitted.
- Report vulnerabilities responsibly while complying with breach notification laws.
- If dealing with cloud-based systems, respect provider terms and avoid illegal access.
- If performing social engineering, ensure no actual personal data is misused.
- Stay updated with NDPA regulations and consult legal professionals if in doubt.