WELCOME!

HACKTHEBOX

What is HTB?

Hack The Box (HTB) is an online platform designed for cybersecurity enthusiasts and professionals to practice and enhance their penetration testing skills. It offers a wide range of challenges, including vulnerable machines that simulate real-world security vulnerabilities, allowing users to develop and refine their hacking techniques in a legal and controlled environment.

Academy

Enterprise

Labs

CTF

Why HTB?

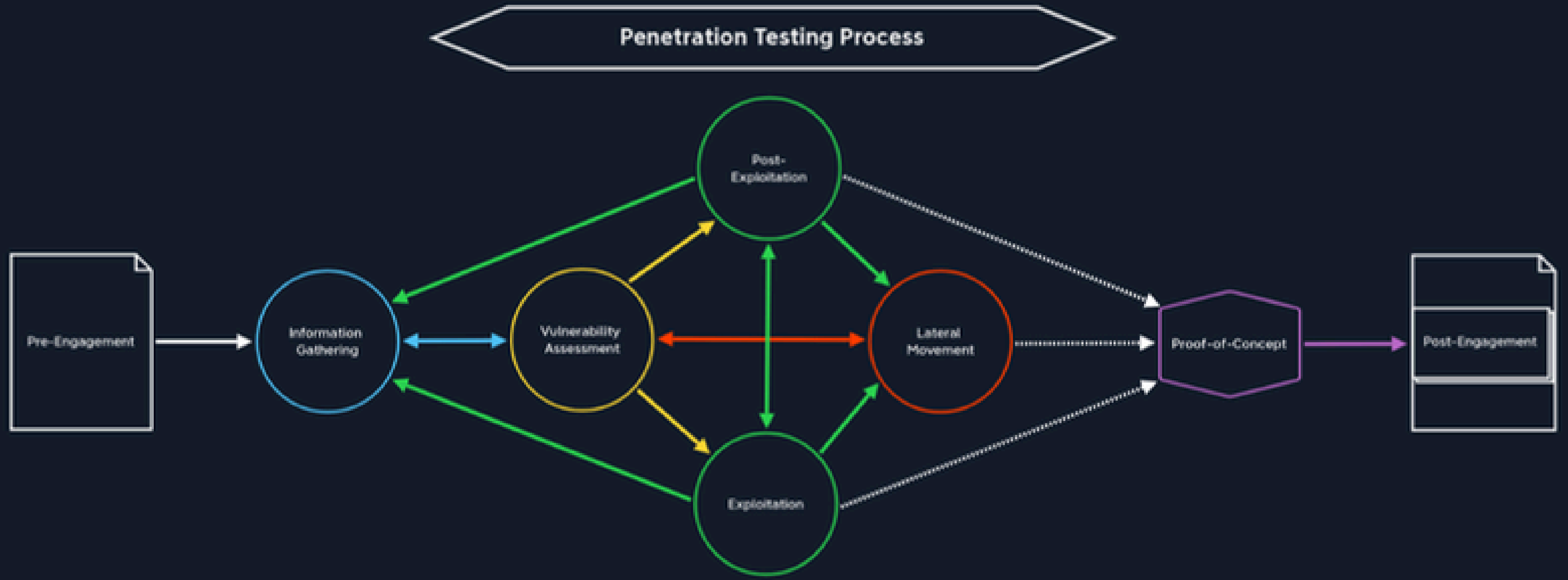
Why HTB?

Because its ✨LEGAL✨

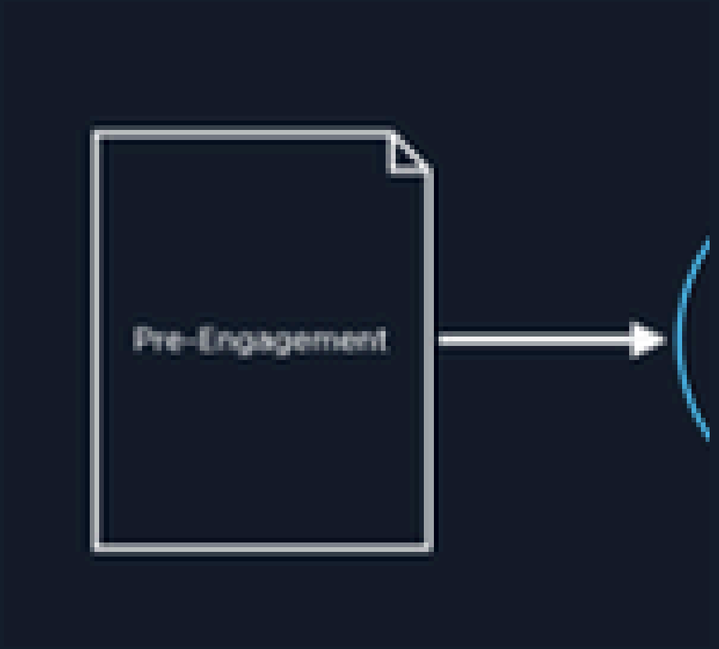
Mindset

Curiosity over fear
Methodical Approach
Never skip the basics
Research and Learn
Document Everything
Enjoy the Process
Persistence

Pentesting Process

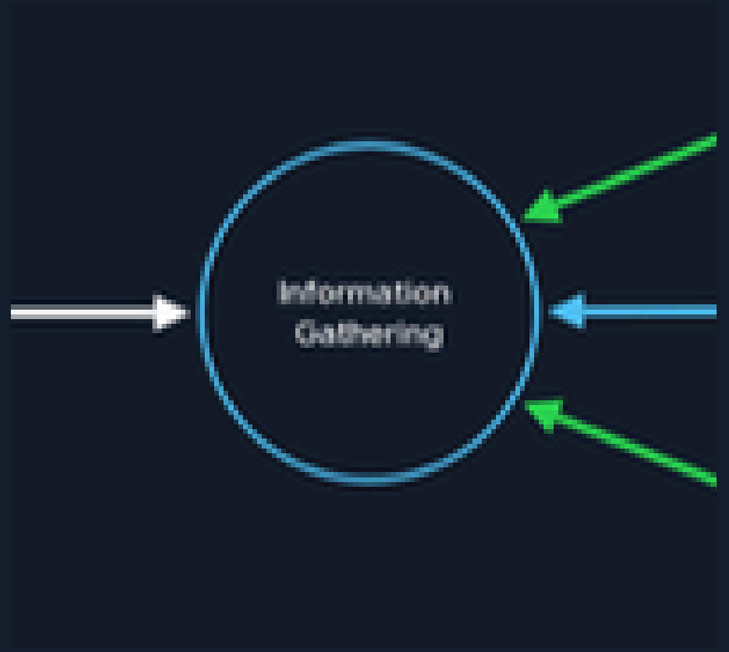

Penetration Testing Process
Pre-Engagement
Information Gathering
Vulnerability Assessment
Post-Exploitation
Exploitation
Lateral Movement
Proof-of-Concept
Post-Engagement

Pre-Engagement



- Main commitments, scope, limitations and agreement are documented
- Contract drawn out between pentester and client

Information Gathering

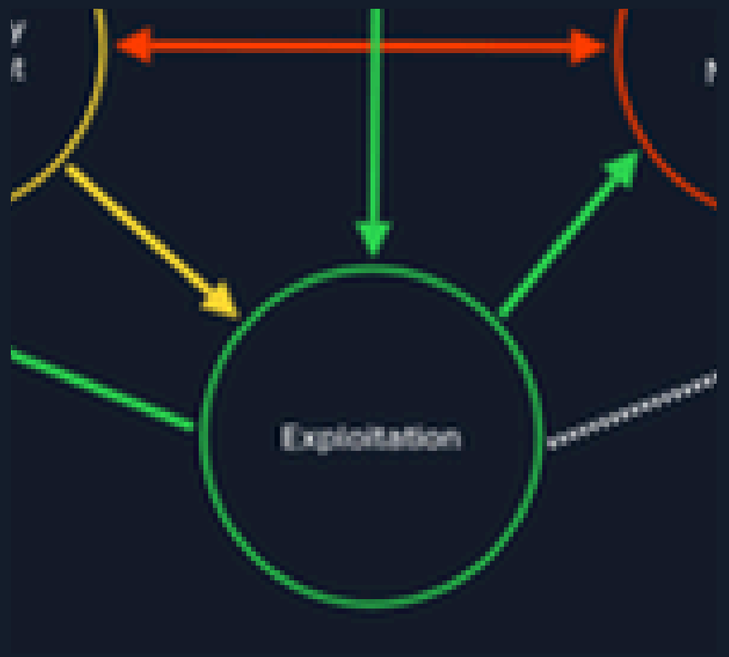


- Essential part in any assesment
- The more information we get, the better our decision are
- Time, passion and commitment are important

Vulnerability Assesment

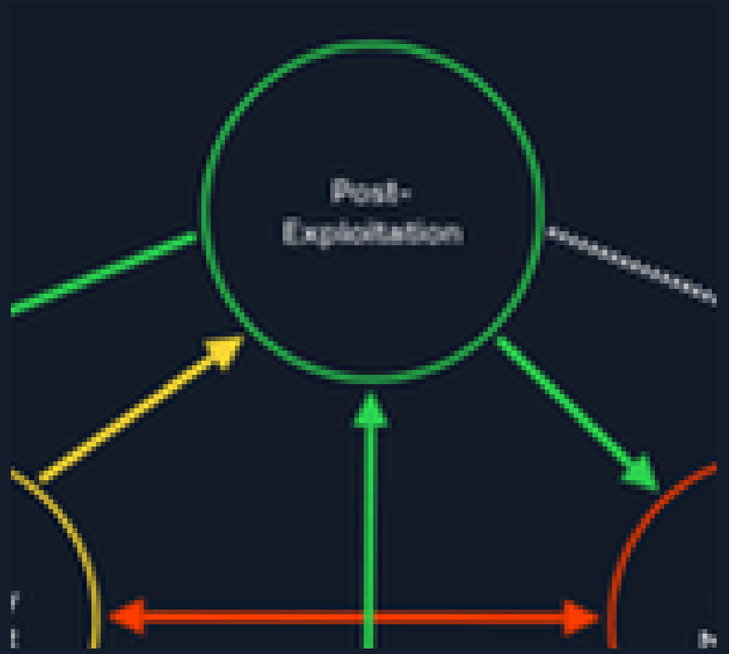
- Identify potential weakness based on the information we gather
- Automated or manual analysis
- Require creativity and deep technical understanding

Exploitation



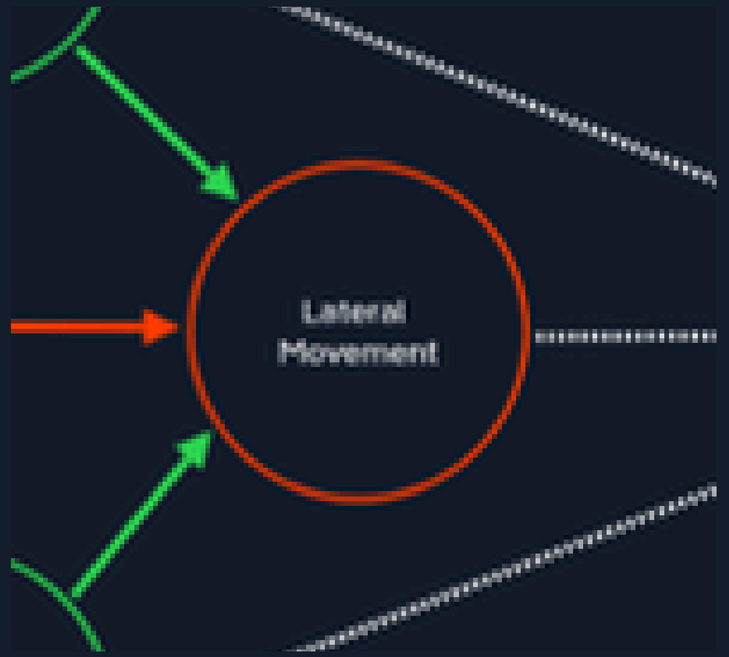
- Performing attack based on the potential vulnerability discovered
- Two distinct areas(in this case) - Network exploitation and web exploitation

Post-Exploitation



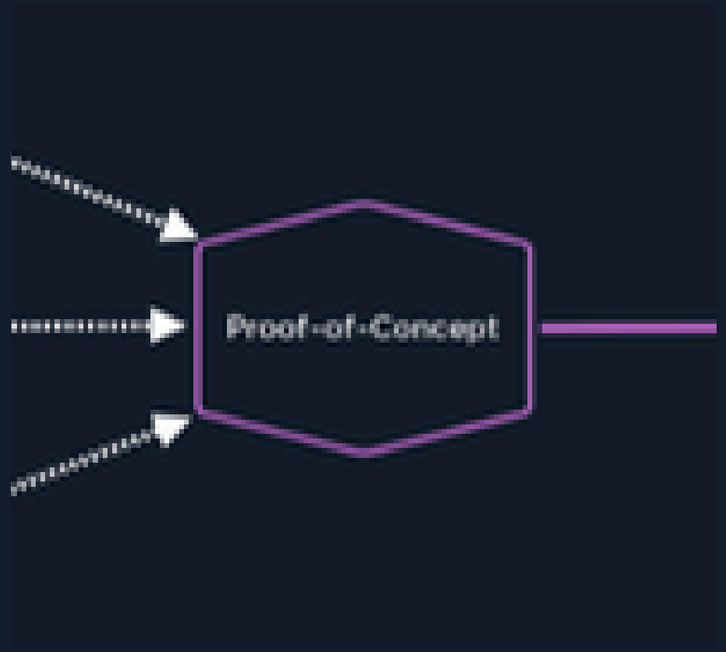
- Gaining further access to a system
- a.k.a Privilege Escalation

Lateral Movement



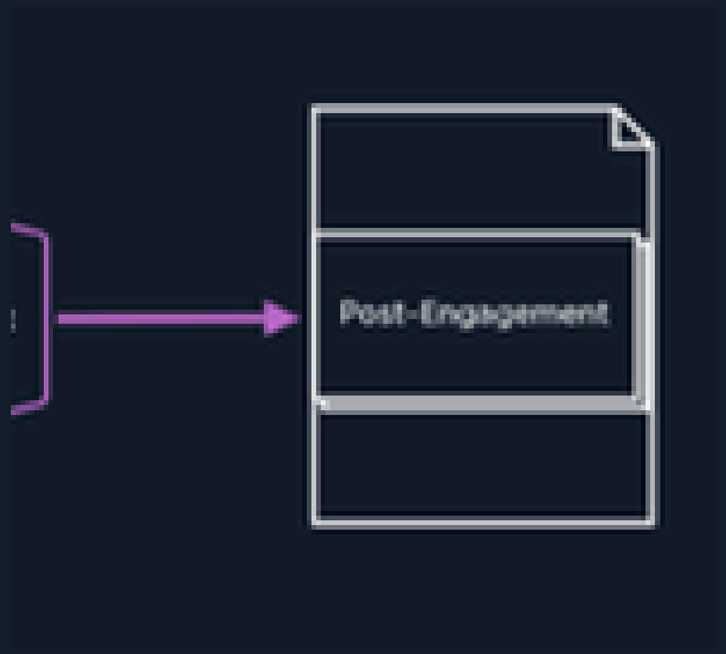
- One of the essential components for moving through a corporate network
- Require access to at least one of the system
- Moving across systems within a network using stolen creds or exploits

Proof-of-Concept



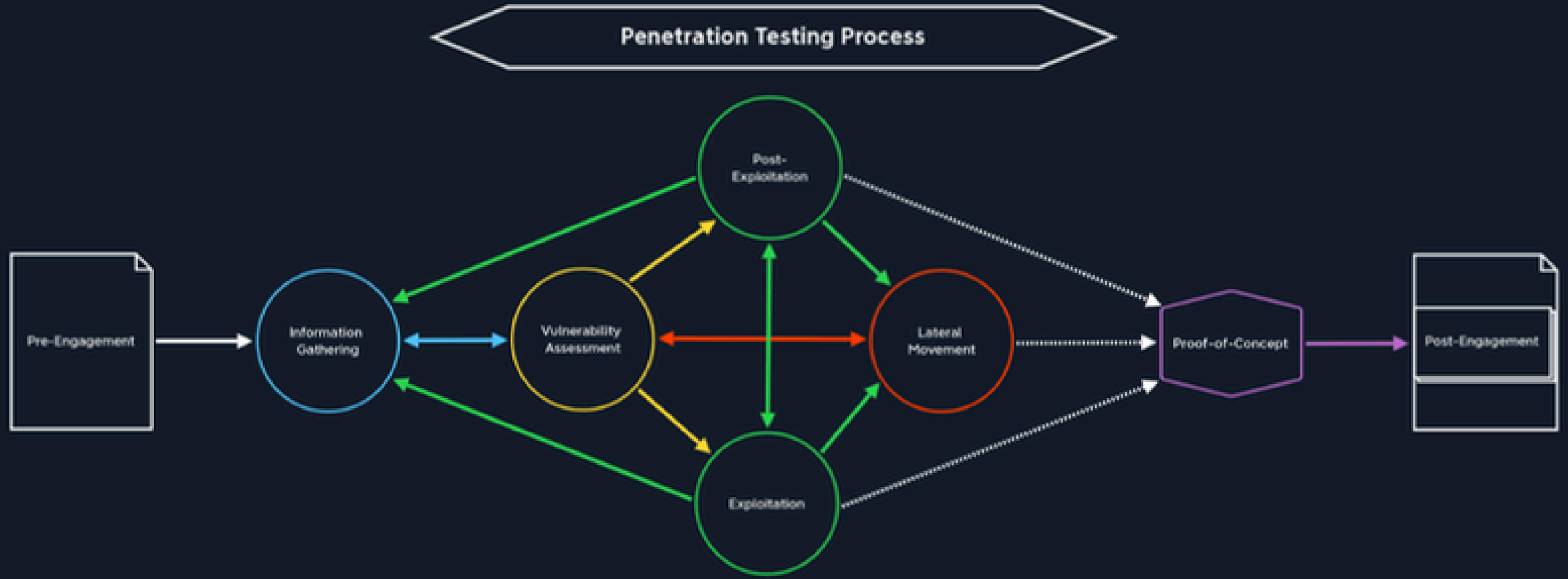
- POC that a vulnerability found exists
- Administrators will try to confirm the vulnerabilities after reported
- Sent along with documentation

Post-Engagement



- Cleaning up the systems we exploit
- E.g. : Remove bind shell that we use
- Note down any system changes, successful exploitation attempts, captured creds and uploaded files
- Provide a comprehensive, well-formatted and neat report to client

Link Between Each Other



How to Approach HTB Machine

Methodology

Reconnaissance
Enumeration
Exploitation
Privilege Escalation

Reconnaissance

Purpose : Gathering initial information

Techniques : Active and passive recon, port scanning, fingerprinting

Tools:

whatweb

nmap

dig

Shodan

Enumeration

Purpose : Extracting more detailed information about discovered services

Techniques : Enumerating directories and files. Identifying misconfig or exploits.

Tools:

gobuster

dirb

nikto

searchsploit

exploitdb

Exploitation

Purpose : Gaining initial access by exploiting vulnerabilities

Techniques : Using known CVE or developing custom exploits.

Tools:

metasploit

sqlmap

burpsuite

msfvenom

exploitdb

Privilege Escalation

Purpose : Elevating access from a lower-privileged user to root/admin

Techniques : Exploiting weak file permissions, SUID binaries, misconfigurations, kernel vulneabilities.

Tools:

LinPEAS

WinPEAS

GTFOBins

SUID3num

BloodHound

PrivescCheck

LETS HACK!