MODULE 1, BOOKLET 1

Ethical hacker

Introduction to Ethical Hacking and Penetration Testing

By BELKHIR Selma

Ethical hacker & penetration testing

-ETHICAL HACKER: A PERSON WHO ACTS AS AN ATTACKER AND EVALUATES THE SECURITY POSTURE OF A COMPUTER NETWORK FOR THE PURPOSE OF MINIMIZING RISK.

-PENETRATION TESTING: ANALYZING THE SECURITY POSTURE OF A NETWORK'S OR SYSTEM'S INFRASTRUCTURE IN AN EFFORT TO IDENTIFY AND POSSIBLY EXPLOIT ANY SECURITY WEAKNESSES FOUND AND THEN DETERMINE IF A COMPROMISE IS POSSIBLE.

Why Do We Need to Do Penetration Testing?

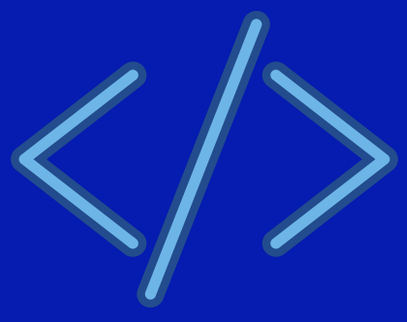
- Identifies potential paths for compromise and validates the effectiveness of defenses like firewalls and IPS.

- Regular testing is essential due to evolving threats and changes in networks.

Threat Actors

-ORGANIZED CRIME : A VERY WELL-FUNDED AND MOTIVATED GROUPS THAT WILL TYPICALLY USE ANY AND ALL OF THE LATEST ATTACK TECHNIQUES. WHETHER THAT IS RANSOMWARE OR DATA THEFT, IF IT CAN BE MONETIZED, ORGANIZED CRIME WILL USE IT.

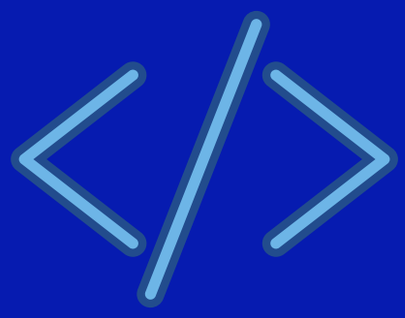
-HACKTIVISTS : THIS TYPE OF THREAT ACTOR IS NOT MOTIVATED BY MONEY. THEY'RE LOOKING TO MAKE A POINT OR TO FURTHER THEIR BELIEFS, USING CYBERCRIME AS THEIR METHOD OF ATTACK.



Threat Actors

-STATE-SPONSORED ATTACKERS : CYBER WAR AND CYBER ESPIONAGE ARE TWO TERMS THAT FIT INTO THIS CATEGORY. MANY GOVERNMENTS AROUND THE WORLD TODAY USE CYBER ATTACKS TO STEAL INFORMATION FROM THEIR OPPONENTS AND CAUSE DISRUPTION.

-INSIDER THREATS : A THREAT THAT COMES FROM INSIDE AN ORGANIZATION. THE MOTIVATIONS OF THESE TYPES OF ACTORS ARE NORMALLY DIFFERENT FROM THOSE OF MANY OF THE OTHER COMMON THREAT ACTORS



Why Methodology Matters in Penetration Testing

Following a methodology for penetration testing helps prevent scope creep and ensures that the methods used are proven and reliable.

By using a known methodology, you can provide documentation of a specialized procedure that has been used by many people.

environmental considerations for the types of penetration tests

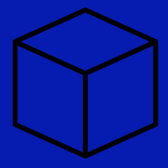
1.NETWORK INFRASTRUCTURE TESTS: ASSESSES SECURITY OF COMPONENTS LIKE FIREWALLS AND AAA SERVERS, MAY INCLUDE WIRELESS TESTS.

2.APPLICATION-BASED TESTS: FOCUSES ON SECURITY FLAWS IN ENTERPRISE APPS, REFERENCING STANDARDS LIKE OWASP.

3.PENETRATION TESTING IN THE CLOUD: INVOLVES SHARED SECURITY RESPONSIBILITIES WITH CLOUD PROVIDERS LIKE AWS, AZURE, AND FOLLOWS CSP GUIDELINES.

Different Types of Penetration Testing

BLACK BOX: MINIMAL INFORMATION IS PROVIDED (LIKE DOMAIN NAMES OR IP ADDRESSES) SIMULATING AN EXTERNAL ATTACKER'S APPROACH.



WHITE BOX: TESTER HAS DETAILED KNOWLEDGE (E.G., NETWORK DIAGRAMS, IP ADDRESSES, CONFIGURATIONS) ALLOWING FOR COMPREHENSIVE INTERNAL ASSESSMENTS.

GRAY BOX: COMBINES ELEMENTS OF BLACK AND WHITE BOX TESTING, WITH PARTIAL ACCESS TO SIMULATE REALISTIC SCENARIOS.

Penetration Testing Standards and Methodologies

- **MITRE ATT&CK:** A framework detailing adversary tactics, techniques, and procedures (TTPs) used in attacks, aiding penetration testers, red teamers, and threat responders.

- **OWASP WSTG:** A comprehensive guide for web application security testing, covering attack vectors like XSS, XXE, CSRF, and SQL injection, and methods for their prevention.

Penetration Testing Standards and Methodologies

- **NIST SP 800-115:** A standard offering guidelines for conducting penetration testing, serving as an industry benchmark for information security testing.

- **OSSTMM:** A repeatable security testing methodology that includes various security testing areas such as operational, physical, wireless, and data networks security.

Penetration Testing Standards and Methodologies

- **PTES:** A seven-phase framework for penetration testing, encompassing pre-engagement, intelligence gathering, exploitation, and reporting, with an emphasis on attack types and tools.

- **ISSAF:** A methodology focusing on stages from information gathering to access maintenance, with additional phases like compromising remote users and covering tracks.

Thank you for your attention. Feel free to leave any comments or questions

By BELKHIR Selma