ETHL 0x00 - Introduction

Il security testing può essere suddiviso in tre distinti aspetti, ciascuno caratterizzato aspetti diversi:

1. ***Vulnerability Assessment***
   Targets: systems (networks, servers, laptops, applications)
   Focus: breadth of vulnerability coverage (typically automated)
   Methodology: primarily automated with manual intervention and triage (false positives) **Limitations**: may not identify specific attack paths leading to critical compromise (we want to cover as much as possible)
2. ***Penetration Testing***
   Targets: systems (networks, servers, laptops, applications)
   Focus: depth and achieving the objective (e.g., capturing the "flag")
   Methodology: exploiting identified vulnerabilities to establish a foothold and reach the objective (possible to use automated in some case)
   Limitations: leveraging the path of least resistance may not uncover alternative attack paths or offer comprehensive system security evaluation
3. ***Red Teaming***
   Targets: Systems, processes, physical security, …
   Focus: We want to emulate real-world attackers, exploiting vulns across various attack vectors
   Methodology: Advanced techniques like social engineering, zero-day exploits, and physical intrusion
   Limitations: May cause disruption to normal operations, operational security and ethical considerations must be addressed

Kill chain & ATT&CK

La ***Kill Chain*** è un framework che permette di visualizzare il percorso dell'attaccante, dalla fase iniziale di ricognizione fino all'esfiltrazione dei dati sensibili o al danneggiamento del sistema. Comprendere ogni fase di questo processo consente di:

- implementare difese mirate per interrompere l'attacco
- valutare il rischio e i possibili percorsi d'attacco in un contesto realistico.

ATT&CK® è l'acronimo di *Adversarial Tactics, Techniques & Common Knowledge* e rappresenta una base di conoscenza e un modello per il comportamento degli avversari nel cyberspazio. Fornisce una tassonomia delle azioni specifiche utilizzate dagli attaccanti, comprensibile sia dal lato offensivo che difensivo della cybersecurity. Inoltre, associa le varie tecniche ai gruppi *APT* (*Advanced Persistent Threat*), permettendo di analizzare e contrastare le minacce in modo più efficace.

Lockheed Martin KC - 7 stages

1. ***Reconnaissance***

   Gli attaccanti raccolgono informazioni sui sistemi target e sulle loro vulnerabilità

   Tecniche: ingegneria sociale, uso di fonti di intelligence aperte (OSINT), scansione di rete

   Metodi: può avvenire online o offline, essere completamente passiva

   Strumenti:

   - **Shodan** (allows you to search for specific types and versions of servers, networking equipment, industrial control systems, and IoT devices).
   - **Censys** focuses on Internet-connected hosts, websites, certificates, and other Internet assets.
   - **VirusTotal** is an online website that provides a virus-scanning service for files using multiple antivirus engines
   - **Have I Been Pwned (HIBP)** tells you if an email address has appeared in a leaked data breach.Google Dorks.
   - **Trasparenza dei certificati X.509** (Può facilitare l'individuazione di domini e sottodomini associati a un'organizzazione. In alcuni casi, se non si conoscono esattamente i sistemi presenti, si può tentare un'enumerazione brute force per scoprirli)

   In alcuni casi, se non si conoscono esattamente i sistemi presenti, si può tentare un'enumerazione brute force per scoprirli

   Esempio: individuazione di domini e sottodomini associati a un'organizzazione tramite la trasparenza dei certificati X.509

2. ***Weaponization***

   Gli attaccanti creano o modificano strumenti malevoli per sfruttare le vulnerabilità individuate

   Tecniche: sviluppo di malware personalizzato, modifica di strumenti esistenti, uso di exploit kit

   Metodi: inserimento di codice malevolo all'interno di un software legittimo di interesse per la vittima

   In alcuni casi, ricerca di vulnerabilità zero-day nei sistemi utilizzati dal bersaglio

   Esempio: inserimento di codice malevolo all'interno di un software legittimo di interesse per la vittima

3. ***Delivery***

   Gli attaccanti consegnano il payload malevolo al sistema target

   Tecniche: email di phishing, siti web dannosi, dispositivi USB infetti, attacchi watering hole

   In alcuni casi, compromissioni nella supply chain

   Esempio: invio di un'email di spear-phishing con un allegato malevolo a un dipendente specifico dell'organizzazione bersaglio

4. ***Exploitation***

   Gli attaccanti sfruttano vulnerabilità nei sistemi, nelle persone o nella sicurezza fisica per ottenere accesso

   Tecniche: escalation dei privilegi, movimento laterale all'interno della rete

   Esempio: navigazione attraverso il network, sfruttando sistemi interconnessi e configurazioni errate per raggiungere dati o risorse di interesse

5. ***Installation***

   Gli attaccanti garantiscono la persistenza installando software e strumenti malevoli

   Tecniche: installazione di una backdoor

   Obiettivo: mantenere l'accesso anche dopo un riavvio del sistema o un'eventuale rilevazione

   Esempio: installazione di una backdoor per ottenere un accesso remoto continuo al sistema compromesso

6. ***Command and Control (C2)***

   Gli attaccanti creano canali di comunicazione, spesso criptati o nascosti, per evitare la rilevazione

   Tecniche: utilizzo di DNS o social media

   Obiettivo: inviare istruzioni ai sistemi infetti per scaricare ulteriore malware, rubare dati, lanciare attacchi o eseguire altre attività dannose

   Esempio: esfiltrazione dei dati trasferendoli all'attaccante tramite i canali di comando e controllo (C2)

7. ***Actions and Objectives***

   Gli attaccanti raggiungono i loro obiettivi

   Tecniche: furto di dati, interruzione dei servizi, installazione di ransomware

   Le azioni specifiche dipendono dalla motivazione e dal bersaglio dell'attacco

   Esempio: furto di dati finanziari sensibili o rilascio di ransomware per estorcere denaro