Indice

Elenco delle figure

CAPITOLO 1

Pre-Exploitation

1.1 Target Scoping

Dal momento che il processo di *Penetration Testing* ha uno scopo puramente didattico non è prevista una fase di accordo tra le parti coinvolte in quanto l'asset da analizzare è una macchina virtuale vulnerabile *by design*. Non vi è, infatti, un cliente dal quale raccogliere requisiti e con il quale definire obiettivi di business e modelli dei costi. Il processo verrà svolto senza particolari vincoli formali relativi all'asset.

1.2 Information Gathering

La caratterizzazione dell'asset da analizzare può generalmente avvenire mediante molteplici *tool* e coinvolgere diversi aspetti dell'asset stesso. Dal momento che si sta trattando una macchina virtuale vulnerabile *by-design* contestualizzata in un'attività progettuale avente uno scopo didattico non risulta utile ricorrere a particolari tecniche *OSINT (Open Source INTelligence)*, né a tecniche volte all'ottenimento di informazioni di routing e record DNS. Sono state, tuttavia, consultate le informazioni di base dell'asset disponibili sulla piattaforma *VulnHub* che mette a disposizione la macchina virtuale. Le informazioni fornite sono le seguenti:

- **Nome della macchina**: *Momentum: 1*;
- **Sistema Operativo**: *Linux*;
- **DHCP Server**: abilitato;
- **Indirizzo IP**: assegnato in automatico.

Non risultano, dunque, note le informazioni relative all'indirizzo IP della macchina né le credenziali di accesso alla stessa.

1.3 Target Discovery

1.4 Target Enumeration

1.5

Bibliografia