



UNIVERSITÀ DEGLI STUDI DI SALERNO

Dipartimento di Informatica

Corso di Laurea Magistrale in Informatica

CORSO DI PENETRATION TESTING
AND ETHICAL HACKING

De-ICE S1.140

STUDENTE

Lorenzo Criscuolo

Matricola: 0522501268

DOCENTE

Prof. Arcangelo Castiglione

Università degli studi di Salerno

Anno Accademico 2022-2023

Indice	i
1 Introduzione	1
1.1 Ambiente utilizzato	2
1.2 Strumenti utilizzati	3

CAPITOLO 1

Introduzione

Il presente documento ha lo scopo di illustrare passo-passo tutte le attività svolte durante il progetto del corso di "*Penetration Testing and Ethical Hacking*". Per lo svolgimento dello stesso è stato necessario scegliere un asset da analizzare e, dunque, è stata scelta una macchina virtuale vulnerabile by-design identificata con il nome **De-ICE S1.140** e indicizzata al seguente indirizzo: <https://www.vulnhub.com/entry/de-ice-s1140,57/>.

L'intera attività progettuale sarà suddivisa in fasi, in modo da emulare nel modo più preciso possibile il lavoro svolto da un hacker etico e per contestualizzare al meglio ogni passo eseguito durante il processo. Le fasi in cui sarà suddivisa l'attività sono:

- **Target Scoping:** in questa fase vengono presi accordi con il proprietario dell'asset da analizzare, definendo limiti riguardo host da analizzare, indirizzi, ecc. e definendo le metodologie da applicare;
- **Information Gathering:** in questa fase si impiegano varie tecniche e strumenti con lo scopo di raccogliere quante più informazioni possibile riguardo l'asset come personale afferente all'organizzazione, indirizzi e-mail, software utilizzati nell'organizzazione (utili per eventuale attività di Social Engineering), infrastruttura di rete, domini DNS e, in generale, ogni informazione che può essere utile per le fasi successive del processo;
- **Target Discovery:** in questa fase vengono impiegate strategie e strumenti attivi e passivi per scansionare la rete (o le sottoreti) per identificare le macchine effettivamente attive nell'asset da analizzare e l'OS che utilizzano;

- **Target Enumeration:** in questa fase viene eseguita una scansione a livello di servizi offerti sulle macchine identificate con lo scopo di capire, appunto, quali servizi vengono offerti e le versioni di questi;
- **Vulnerability mapping:** in questa fase si cerca di capire quali sono le eventuali vulnerabilità di cui sono affette le versioni dei servizi identificati nella fase precedente;
- (CONTINUA)

1.1 Ambiente utilizzato

Essendo che l'asset da analizzare è una *macchina virtuale* dovrà essere necessariamente utilizzato un *ambiente di virtualizzazione* appropriato. Per questa ragione, è stato utilizzato **Oracle VM VirtualBox 7.0.8** per creare un *ambiente di virtualizzazione* sul quale poi effettuare l'intero processo. Oltre a creare l'ambiente di esecuzione della macchina è stato necessario eseguire un altro passo, ovvero la *creazione di una rete* con la quale poi essere in grado di comunicare con l'asset stesso. Fortunatamente, *VirtualBox* rende disponibile la funzionalità di *NAT* e, infatti, in maniera molto semplice è possibile creare una **rete NAT ad-hoc** sulla quale collegare l'asset da analizzare (ed eventuali altre macchine). Per realizzare questa rete *NAT*, tutto quello che bisogna fare è:

1. Aprire il pannello degli strumenti di VirtualBox;
2. Selezionare il sotto-menù rete;
3. All'interno della pagina, selezionare il pannello "Reti con NAT";
4. Cliccare il pulsante per la creazione di una nuova rete ed impostare i parametri desiderati.

Per essere conformi alle istruzioni fornite dal docente durante le lezioni riguardo la definizione dell'ambiente, i parametri della rete saranno i seguenti:

- **Nome della rete:** Corso
- **Spazio di indirizzamento:** 10.0.2.0/24

Come ultimo passo, per fare in modo che l'asset (e altre eventuali macchine) utilizzi questa rete creata *ad-hoc*, basta aprire le impostazioni di rete della macchina e impostare come

rete da utilizzare (nel rispettivo menù a riguardo) la rete NAT appena creata identificata dal nome scelto in precedenza.

Il risultato che si ottiene quando si configurano in questo modo l'asset e VirtualBox è il seguente schema di rete:

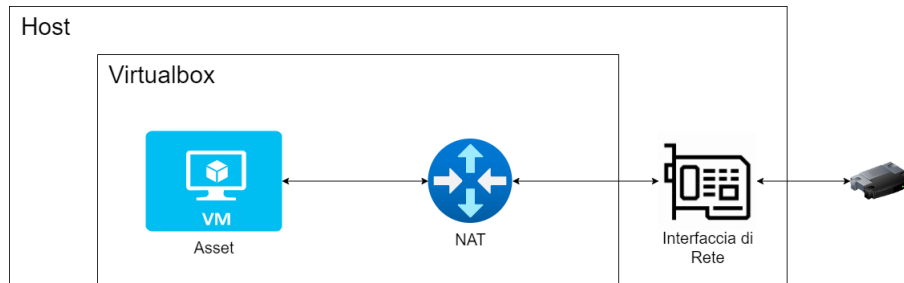


Figura 1.1: Infrastruttura di rete

1.2 Strumenti utilizzati

Per proseguire con l'analisi dell'asset, è necessario ottenere strumenti appositi che permettano di realizzare scansioni, mapping di vulnerabilità, ecc. Visto che, come già detto in precedenza, l'asset è una *macchina virtuale* che sarà eseguita in un *ambiente di virtualizzazione* e all'interno di una *rete virtuale con NAT*, il modo più semplice per analizzare l'asset è quella di utilizzare una macchina virtuale realizzata apposta per questo scopo. A tal proposito, si è scelto di utilizzare una macchina virtuale molto popolare chiamata **Kali Linux** (in particolare la versione di riferimento **2023.1**) che viene distribuito con una suite di strumenti pronti all'uso per effettuare attività di Penetration Testing, Digital Forensics e altre simili. A questo punto, essendo che anche **Kali Linux** è una macchina virtuale che viene eseguita all'interno di *VirtualBox*, verrà configurata anch'essa in modo tale che si colleghi alla *rete con NAT* creata in precedenza. Otteniamo così il seguente schema:

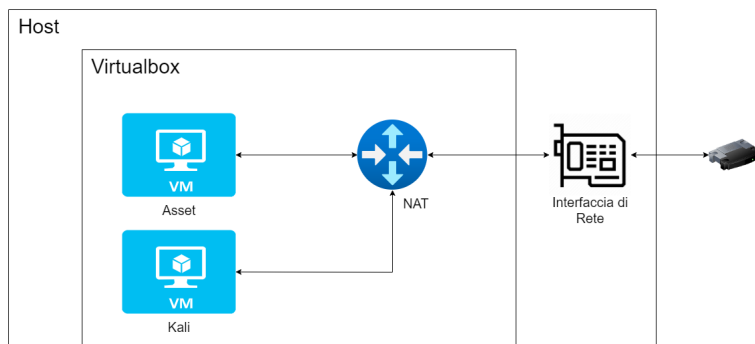


Figura 1.2: Infrastruttura di rete con Kali