



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: Metodologia di Testing

STUDENTE

Lorenzo Criscuolo

Matricola: 0522501268

DOCENTE

Prof. **Arcangelo Castiglione**

Università degli studi di Salerno

Anno Accademico 2022-2023

<b>Indice</b>	<b>i</b>
<b>1 Introduzione</b>	<b>1</b>
1.1 Ambiente utilizzato . . . . .	2
1.2 Strumenti utilizzati . . . . .	3
<b>2 Pre-Exploitation</b>	<b>4</b>
2.1 Target Scoping . . . . .	4
2.2 Information Gathering . . . . .	5
2.3 Target Discovery . . . . .	6
2.4 Target Enumeration . . . . .	6

# 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.

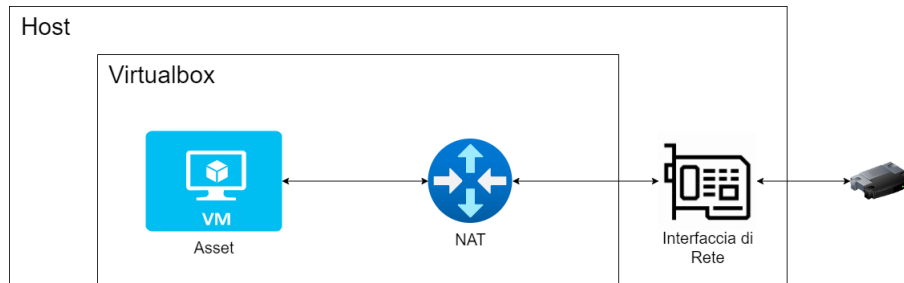
Per essere conformi alle istruzioni fornite dal docente durante le lezioni riguardo la definizione dell'ambiente, i parametri della rete saranno i seguenti:

- **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.

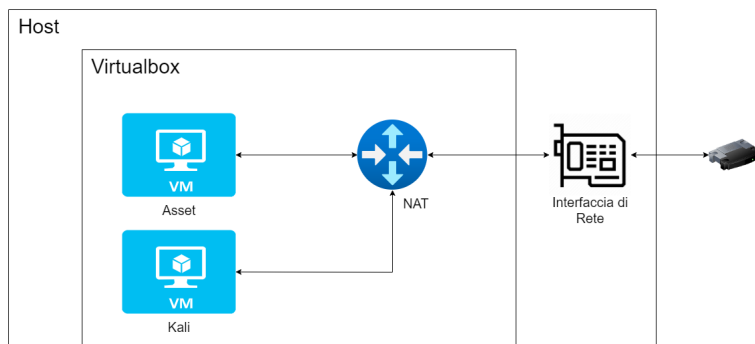
Il risultato che si ottiene quando si configurano in questo modo l'asset e VirtualBox è il seguente schema di rete:



**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

### 2.1 Target Scoping

In questa fase bisogna stipulare un accordo tra le parti (responsabile dell'asset e pentester) in modo da definire vincoli, limiti, responsabilità legali in caso di eventuali problemi, accordo di non divulgazione, ecc. Tuttavia, possiamo fare le seguenti osservazioni:

- L'asset da analizzare è pubblicamente disponibile e realizzato appositamente per essere analizzato, ossia vulnerabile by-design;
- Tutta l'analisi avviene in un ambiente virtualizzato all'interno della macchina in possesso al Penetration Tester;
- Lo scopo dell'analisi è puramente didattico, in quanto realizzato in un contesto universitario e, più precisamente, come progetto del corso "Penetration Testing and Ethical Hacking";
- Tutti gli strumenti utilizzati e le fonti consultate sono pubblicamente disponibili e accessibili o, in generale, sono accessibili tramite piani gratuiti e quindi senza costi da sostenere.

In conclusione, come si può notare dalle precedenti osservazioni, questa fase può essere tranquillamente saltata visto che non ci sono parti con cui prendere accordi e non possono esserci problematiche di tipo legale dal momento che l'ambiente è totalmente simulato.

## 2.2 Information Gathering

Durante questa fase, l'obiettivo è quello di trovare più informazioni possibili riguardo l'asset scelto e, essendo che l'asset è una macchina virtuale che viene eseguita in un *ambiente virtualizzato* e in una *rete con NAT virtuale* (come illustrato nell'introduzione), si eviteranno fonti e tool che raccolgono informazioni riguardo persone afferenti all'organizzazione dell'asset, indirizzi e-mail, analisi di record DNS, informazioni di routing e così via. A questo punto, l'unica tecnica che ha senso utilizzare (e che è stata effettivamente utilizzata) è **OSINT** (*Open Source INTelligence*), con cui si cercherà di individuare nomi utente, password, indirizzo IP, ecc. Tutto questo, ovviamente, evitando di consultare fonti dove sono presenti Walkthrough e guide per evitare di vanificare il contributo didattico del processo.

Come primo passo, è stata consultata la pagina di Vulnhub sulla quale sono riportate varie informazioni riguardo la macchina virtuale scelta "**De-ICE S1.140**" e, all'interno della pagina, sono state trovate le seguenti informazioni:

- Informazioni riguardo il **rilascio**, ovvero autore, data, sorgente e valore hash della macchina. Queste informazioni, tuttavia, non sembrano essere utili per il processo;
- Una **descrizione** molto ad alto livello della macchina. Anche qui non viene rilasciata alcuna informazione utile come servizi esposti dalla macchina o credenziali di accesso alla macchina (anche non privilegiate). Infatti, attualmente, se avviamo la macchina non possiamo fare nulla tramite *interazione diretta* in quanto **non abbiamo nessuna credenziale di accesso**;
- Informazioni riguardo la configurazione dell'**indirizzo di rete**. Questa informazione è molto utile perché ci rivela che la macchina **non è configurata per lavorare con un indirizzo IP specifico** ma lo ottiene in maniera automatica grazie al servizio **DHCP**. Questo ci fa subito capire che all'interno della rete con NAT non avremo problemi di indirizzamento ma, sfortunatamente, questo significa che non conosciamo apriori l'indirizzo della macchina (sappiamo solo che sarà all'interno della rete *10.0.2.0/24*) ma dovremo ricavarcelo in maniera indiretta visto che *VirtualBox* non fornisce un metodo diretto di ottenimento degli indirizzi IP e **non abbiamo accesso alla macchina**;
- Informazioni riguardo il **sistema operativo**. Altra informazione molto utile in quanto adesso sappiamo che l'asset è un sistema Linux e questo ci permetterà di risparmiare tempo in fasi avanzate perché possiamo restringere il campo delle scansioni solo a

sistemi Linux, escludendo tutti gli altri. Tuttavia, non sappiamo ancora la versione precisa del kernel e quindi dobbiamo ricavarla successivamente;

Andando più a fondo nella pagina si può ricavare l'indirizzo del **sito web del creatore** dell'asset e il **link di download della macchina** ma, sfortunatamente, entrambi i link **non sono più attivi**. Consultando il motore di ricerca Google, semplicemente ricercando il nome dell'organizzazione trovato sulla pagina, è possibile risalire al rispettivo account Twitter e si nota che quest'ultimo non è attivo all'incirca dal 2020. Per questa ragione, è sembrato opportuno accedere al servizio *WaybackMachine* offerto da **Archive.org** per visitare versioni precedenti del sito dell'organizzazione nella speranza di trovare altre informazioni utili. Fortunatamente, grazie a questo servizio è stato possibile accedere ad uno *snapshot* risalente al 2021 dal quale è stato anche possibile effettuare il download della macchina. Ad ogni modo, anche accedendo al sito e, in particolare, alla pagina di download, non sono state trovate informazioni rilevanti come credenziali, porte aperte, schemi di naming, ecc.

## 2.3 Target Discovery

## 2.4 Target Enumeration