Report Tecnico

Task-Tech: Analisi di Sicurezza del Sito Web

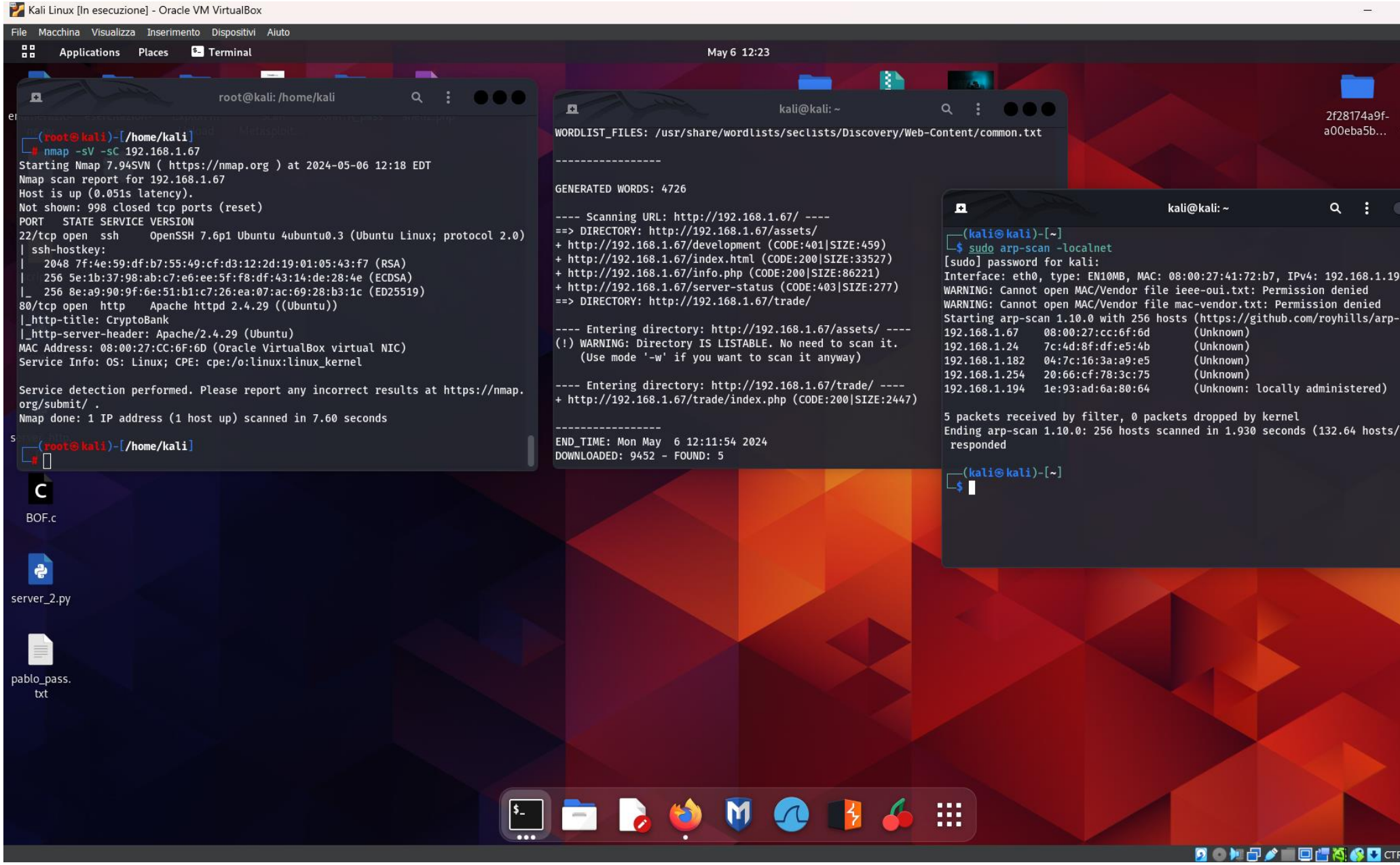
Introduzione: Per il compito assegnato, ho condotto un'analisi approfondita della sicurezza del sito web fornito, al fine di identificare potenziali vulnerabilità e punti deboli che potrebbero essere sfruttati da attaccanti esterni.

Metodologia:

1. **Scansione ARP per individuare l'host attivo:** Inizialmente, ho eseguito una scansione ARP sulla rete per individuare l'host attivo. Questo passaggio è essenziale per identificare i dispositivi attivi nella rete e stabilire una connessione con il server web target.
2. **Scansione del Sito Web con Nmap:** Dopo aver identificato l'host, ho eseguito una scansione del sito web utilizzando Nmap per rilevare i servizi in ascolto sul server. La scansione ha rivelato che i principali servizi in esecuzione sono SSH e HTTP.
3. **Analisi dei Servizi SSH:** Utilizzando la scansione Nmap con l'opzione **-sC**, ho individuato le chiavi SSH RSA, ECDSA e ED25519 associate al servizio SSH della macchina target.
4. **Tentativi di Brute Force con Hydra:** Nonostante gli sforzi, inclusi tentativi di autenticazione con brute force a dizionario utilizzando Hydra, non sono riuscito ad autenticarmi con successo al servizio SSH utilizzando i nomi utente e le password trovati.
5. **Enumerazione delle Directory del Sito Web:** Successivamente, ho eseguito un'enumerazione delle directory del sito web al fine di individuare eventuali punti deboli o directory nascoste. Durante questo processo, ho notato una directory particolare, "/development", che ha attirato la mia attenzione come potenziale fonte di informazioni sensibili.

Risultati e Conclusioni:

- La scansione iniziale ha permesso di individuare l'host attivo e i servizi in esecuzione sul server.
- L'enumerazione delle directory del sito web ha rivelato la presenza della directory /development, che potrebbe contenere informazioni sensibili.
- Nonostante i tentativi di enumerazione dei nomi utente, non è stato possibile ottenere accesso alla directory /development.
- Nonostante i tentativi di autenticazione con brute force, non è stato possibile ottenere accesso al servizio SSH utilizzando i nomi utente e le password trovati.


Kali Linux [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Applications Places Terminal
May 6 12:23
root@kali: /home/kali
(root㉿kali)-[/home/kali]
nmap -sV -sC 192.168.1.67
Starting Nmap 7.94SVN (https://nmap.org) at 2024-05-06 12:18 EDT
Nmap scan report for 192.168.1.67
Host is up (0.051s latency).
Not shown: 998 closed tcp ports (reset)
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 2048 7f:4e:59:df:b7:55:49:cf:d3:12:2d:19:01:05:43:f7 (RSA)
| 256 5e:1b:37:98:ab:c7:e6:ee:5f:f8:df:43:14:de:28:4e (ECDSA)
|_ 256 8e:a9:90:9f:6e:51:b1:c7:26:ea:07:ac:69:28:b3:1c (ED25519)
80/tcp open http Apache httpd 2.4.29 ((Ubuntu))
|_http-title: CryptoBank
|_http-server-header: Apache/2.4.29 (Ubuntu)
MAC Address: 08:00:27:CC:6F:6D (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.60 seconds
(root㉿kali)-[/home/kali]
#
kali@kali: ~
WORDLIST_FILES: /usr/share/wordlists/seclists/Discovery/Web-Content/common.txt
GENERATED WORDS: 4726
---- Scanning URL: http://192.168.1.67/ ----
==> DIRECTORY: http://192.168.1.67/assets/
+ http://192.168.1.67/development (CODE:401|SIZE:459)
+ http://192.168.1.67/index.html (CODE:200|SIZE:33527)
+ http://192.168.1.67/info.php (CODE:200|SIZE:86221)
+ http://192.168.1.67/server-status (CODE:403|SIZE:277)
==> DIRECTORY: http://192.168.1.67/trade/
---- Entering directory: http://192.168.1.67/assets/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)
---- Entering directory: http://192.168.1.67/trade/ ----
+ http://192.168.1.67/trade/index.php (CODE:200|SIZE:2447)
END_TIME: Mon May 6 12:11:54 2024
DOWNLOADED: 9452 - FOUND: 5
kali@kali: ~
(kali㉿kali)-[~]
$ sudo arp-scan -localnet
[sudo] password for kali:
Interface: eth0, type: EN10MB, MAC: 08:00:27:41:72:b7, IPv4: 192.168.1.19
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-
192.168.1.67 08:00:27:cc:6f:6d (Unknown)
192.168.1.24 7c:4d:8f:df:e5:4b (Unknown)
192.168.1.182 04:7c:16:3a:a9:e5 (Unknown)
192.168.1.254 20:66:cf:78:3c:75 (Unknown)
192.168.1.194 1e:93:ad:6a:80:64 (Unknown: locally administered)
5 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.930 seconds (132.64 hosts/
responded
(kali㉿kali)-[~]
$
2f28174a9f-a00eba5b...
BOF.c
server_2.py
pablo_pass.txt