Introduzione
Questa esercitazione ha avuto come obiettivo la familiarizzazione con Kali Linux, la gestione degli utenti del sistema, la configurazione di servizi di rete e l'utilizzo di strumenti di penetration testing per verificare la sicurezza delle credenziali di autenticazione. L'attività si è concentrata principalmente sulla creazione di un ambiente controllato e sul test delle sue vulnerabilità utilizzando lo strumento Hydra.

Configurazione Iniziale del Sistema

Creazione di un Nuovo Utente
Il primo passo dell'esercitazione è stato creare un nuovo utente sul sistema Kali Linux:

```bash
sudo adduser test_user
```

Durante il processo di creazione, è stata impostata la password "testpass" per l'utente. Questa combinazione username/password rappresenta una credenziale debole che sarà poi oggetto di test con Hydra.

La corretta creazione dell'utente è stata verificata con il comando:

```bash
grep test_user /etc/passwd
```

Il risultato ottenuto:
```
test_user:x:1001:1001::/home/test_user:/bin/sh
```

Questo output conferma che l'utente è stato creato correttamente con UID e GID 1001, home directory in `/home/test_user` e shell predefinita `/bin/sh`.

Configurazione del Servizio SSH
Successivamente, è stato attivato il servizio SSH sul sistema:

```bash
sudo service ssh start
```

Il file di configurazione del servizio SSH è stato identificato in `/etc/ssh/sshd_config`. Sebbene l'esercizio menzionasse la possibilità di modificare vari parametri (come l'abilitazione dell'accesso root o il cambio della porta di ascolto), non sono state apportate modifiche alla configurazione predefinita come specificato nelle istruzioni.

Configurazione del Servizio FTP

Per la seconda parte dell'esercitazione, è stato scelto di configurare un servizio FTP come obiettivo per i test di penetrazione. Il servizio vsftpd è stato installato con:

```bash
sudo apt install vsftpd
```

E avviato con:

```bash
sudo service vsftpd start
```

La configurazione predefinita di vsftpd permette l'autenticazione degli utenti locali del sistema, rendendo possibile l'accesso dell'utente test_user precedentemente creato.

Test di Penetrazione con Hydra
Per completare l'esercitazione in tempi ragionevole, ho scelto di creare dizionari personalizzati di dimensioni ridotte:

1. Creazione di un file di dizionario per gli username:
```bash
echo "test_user" > users.txt
```

2. Il file è stato poi esteso con un editor di testo (nano) per includere altri username comuni:
```
test_user
admin
root
user
guest
ftp
administrator
webmaster
support
backup
```

3. Creazione di un file di dizionario per le password:
```bash
echo "testpass" > passwords.txt
```

4. Anche questo file è stato esteso per includere password comuni:
```
testpass
password
admin
123456
qwerty
welcome
abc123
letmein
admin123
passw0rd
```

Esecuzione dell'Attacco
Con i dizionari personalizzati pronti, è stato eseguito Hydra per tentare il brute force dell'autenticazione FTP:

```bash
hydra -L users.txt -P passwords.txt 192.168.60.3 -t4 ftp
```

Il parametro `-t4` limita il numero di tentativi paralleli a 4, riducendo il carico sul server ma aumentando il tempo necessario per completare il test.

L'esecuzione di Hydra con questi parametri ha permesso di testare tutte le combinazioni di username e password presenti nei file dizionario, con l'obiettivo di identificare le credenziali valide per l'accesso al servizio FTP.

Analisi di Sicurezza

Vulnerabilità Identificate
1. **Credenziali deboli**: L'utente test_user con password "testpass" rappresenta una combinazione facilmente indovinabile.
2. **Servizi esposti**: Sia SSH che FTP sono servizi che, se non adeguatamente configurati, possono rappresentare punti di ingresso per attacchi.
3. **Autenticazione basata su password**: L'utilizzo della sola autenticazione con password, senza metodi aggiuntivi come chiavi SSH o autenticazione a due fattori, aumenta il rischio di accessi non autorizzati.

Considerazioni sulla Mitigazione
1.**Politiche di password robuste**: Implementare requisiti di complessità per le password e rotazione periodica.
2. **Limitazione degli accessi****: Configurare i servizi per accettare connessioni solo da indirizzi IP specifici quando possibile.
3. **Autenticazione avanzata**: Per SSH, utilizzare l'autenticazione a chiave pubblica invece delle password.
4. **Monitoraggio**: Implementare sistemi di monitoraggio per rilevare tentativi di brute force.
5. **Aggiornamenti**: Mantenere i servizi aggiornati per prevenire vulnerabilità note.

Conclusioni
L'esercitazione ha fornito una comprensione pratica delle tecniche base di penetration testing e dell'importanza di configurazioni sicure nei servizi di rete. Ha dimostrato come strumenti come Hydra possano essere utilizzati sia da amministratori di sistema per verificare la sicurezza delle proprie installazioni, sia da potenziali attaccanti per compromettere sistemi con configurazioni deboli.

Il lavoro svolto ha evidenziato come anche in un ambiente controllato e con un numero limitato di tentativi, l'utilizzo di credenziali deboli possa rapidamente portare alla compromissione di un sistema. Questa consapevolezza è fondamentale per la progettazione e la manutenzione di infrastrutture IT sicure.