Ecco una guida dettagliata passo per passo per rendere sicuro un server IIS (Internet Information Services) su Windows Web Server senza utilizzare HTTPS. Ogni passaggio è spiegato chiaramente per facilitare l'implementazione.

---

1. Aggiorna il Sistema Operativo e IIS

Motivo: Gli aggiornamenti forniscono patch per vulnerabilità conosciute.

1. **Esegui Windows Update**:
    - Apri il menu **Start** → **Impostazioni** → **Windows Update**.
    - Clicca su **Verifica aggiornamenti** e installa eventuali patch disponibili.
2. **Aggiorna IIS**:
    - IIS viene aggiornato tramite Windows Update. Controlla che la versione installata sia la più recente usando:
        - Vai su **Pannello di controllo** → **Programmi** → **Attiva o disattiva funzionalità di Windows**.
        - Espandi la voce **Internet Information Services** e verifica i componenti installati.

---

2. Disabilita Servizi Non Necessari

Motivo: Ridurre la superficie d'attacco limitando i servizi esposti.

A. Disabilita i Moduli Non Necessari di IIS

1. Apri **IIS Manager**:
    - Premi **Win + R**, digita `inetmgr` e premi **Invio**.
2. Seleziona il server nella lista a sinistra.
3. Vai su **Gestione Moduli** nella sezione centrale.
4. Rimuovi i moduli non utilizzati (ad esempio, FTP o WebDAV):
    - Clicca sul modulo → **Rimuovi** → Conferma.

B. Disabilita Servizi di Windows Inutili

1. Premi **Win + R**, digita `services.msc` e premi **Invio**.
2. Cerca i seguenti servizi e imposta il tipo di avvio su **Disabilitato** se non necessari:
    - **SSDP Discovery**.
    - **Function Discovery Resource Publication**.
    - **Print Spooler** (se il server non è una stampante).
    - **Remote Desktop Services** (se non usato).

---

3. Configura il Firewall

Motivo: Limitare il traffico alle porte necessarie.

A. Permetti Solo il Traffico HTTP (porta 80)

1. Apri **Firewall di Windows**:
    - Premi **Win + R**, digita `wf.msc` e premi **Invio**.
2. Crea una nuova regola per HTTP:
    - **Regole in entrata** → **Nuova regola**.
    - Tipo di regola: **Porta**.

- Seleziona **TCP**, specifica **porta 80**.
- Azione: **Consenti la connessione**.
- Nome: "Allow HTTP Traffic".

B. Blocca ICMP (Ping)

Motivo: Riduce la possibilità di rilevare il server tramite scansioni di rete.

1. Apri PowerShell come amministratore.
2. Esegui il comando:

```
Set-NetFirewallRule -DisplayName "File and Printer Sharing (Echo Request - ICMPv4-In)" -Enabled False
```

---

4. Configura Header HTTP per la Sicurezza

Motivo: Proteggere il server da attacchi come XSS, clickjacking e sniffing.

1. Apri il file di configurazione del sito **web.config**.
   - Si trova nella directory root del sito (es. `C:\inetpub\wwwroot`).
2. Aggiungi o modifica la sezione `<system.webServer>` come segue:

```
<configuration>
  <system.webServer>
    <httpProtocol>
      <customHeaders>
        <add name="X-Content-Type-Options" value="nosniff" />
        <add name="X-XSS-Protection" value="1; mode=block" />
        <add name="X-Frame-Options" value="DENY" />
      </customHeaders>
    </httpProtocol>
  </system.webServer>
</configuration>
```

3. Salva il file e riavvia IIS:
   - Esegui `iisreset` in PowerShell o Prompt dei comandi.

---

5. Nascondi Dettagli del Server

Motivo: Prevenire la divulgazione di informazioni sulla versione del server.

1. **Disabilita l'header "Server"**:
   - Apri il registro di sistema (`regedit`).
   - Vai a:

     ```
     HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\HTTP\Parameters
     ```

   - Crea un nuovo valore DWORD:
     - Nome: `DisableServerHeader`.
     - Valore: `1`.
   - Riavvia il server IIS:

```
iisreset
```

---

6. Disabilita i Metodi HTTP Non Sicuri

Motivo: Prevenire l'uso di metodi come `OPTIONS`, `TRACE`, `PUT`, e `DELETE`.

1. Apri il file **web.config** del tuo sito.
2. Aggiungi o modifica la sezione `<requestFiltering>`:

```
<configuration>
  <system.webServer>
    <security>
      <requestFiltering>
        <verbs>
          <add verb="OPTIONS" allowed="false" />
          <add verb="TRACE" allowed="false" />
          <add verb="PUT" allowed="false" />
          <add verb="DELETE" allowed="false" />
        </verbs>
      </requestFiltering>
    </security>
  </system.webServer>
</configuration>
```

3. Salva il file e riavvia IIS.

---

7. Proteggi i File e le Cartelle

Motivo: Limitare l'accesso non autorizzato ai file.

1. Vai alla directory root del sito (es. `C:\inetpub\wwwroot`).
2. Clicca con il tasto destro → **Proprietà** → **Sicurezza**.
3. Rimuovi utenti o gruppi non necessari e assegna i seguenti permessi:
   - **IIS_IUSRS**: Lettura ed esecuzione.
   - **Administrator**: Controllo completo.

---

8. Abilita il Monitoraggio e il Logging

Motivo: Identificare tentativi di attacco o comportamenti sospetti.

1. Apri **IIS Manager**.
2. Seleziona il tuo sito → **Logging**.
3. Configura:
   - Formato log: **W3C**.
   - Directory dei log: Usa una posizione sicura (es. `D:\Logs`).
4. Controlla regolarmente i file di log per rilevare attività anomale.

---

9. Limita la Velocità delle Richieste

Motivo: Prevenire attacchi DoS/DDoS.

1. Apri **IIS Manager**.
2. Vai a **Dynamic IP Restrictions** (installalo tramite Windows Features se non disponibile):
    - Limita il numero di richieste per IP in un certo intervallo di tempo.
3. Configura blocchi temporanei o permanenti per IP che superano la soglia.

---

10. Testa il Server con Nmap

Motivo: Verifica le configurazioni di sicurezza.

1. Esegui una scansione di base:

```
nmap -sV -O -p 80 <IP del server>
```

2. Controlla che:
    - Non vengano esposti dettagli sulla versione di IIS.
    - I metodi HTTP non sicuri siano disabilitati.
    - Il server risponda solo alla porta 80.

Seguendo questi passaggi, il tuo server IIS sarà significativamente più sicuro, anche senza HTTPS. Tuttavia, l'uso di HTTPS rimane altamente consigliato per proteggere i dati durante il transito.