Relazione: Sicurezza di un Server IIS

Per mettere in sicurezza un server IIS, sono stati eseguiti i seguenti passaggi:

1. Disabilitazione di servizi e moduli non necessari, come WebDAV e FTP.
2. Configurazione del firewall per consentire solo il traffico HTTP sulla porta 80 e bloccare ICMP (ping).
3. Implementazione di header HTTP (X-Content-Type-Options, X-XSS-Protection,

X-Frame-Options) per mitigare attacchi XSS e clickjacking.

1. Nascondere l'header "Server" per evitare la divulgazione di informazioni sulla versione di IIS.
2. Disabilitazione di metodi HTTP non sicuri come OPTIONS, TRACE, PUT e DELETE.
3. Protezione dei file e delle cartelle del sito, limitando i permessi a utenti essenziali.
4. Test della sicurezza con Nmap per confermare che solo la porta 80 sia aperta e che non siano esposte vulnerabilità.

**Comandi di Kali Linux per il Test**

1. nmap -sV -p 80 <IP>: per verificare i servizi attivi sulla porta HTTP.
2. nmap -p- <IP>: per scansionare tutte le porte e verificare che solo la porta 80 sia aperta.
3. nmap --script vuln -p 80 <IP>: per controllare vulnerabilità note nel server.
4. Questi test hanno confermato che il server è configurato correttamente e sicuro.