1)

XSS
Per prevenire un attacco XSS bisogna sanitizzare gli input di pagina web o di un'applicazione web.
Il tutto dipende comunque dal sottogenere di vulnerabilita' XSS:input ed programming framework.
*Step 1 training e consapevolezza
Per tenere in sicurezza l'applicazione web,ogni persona coinvolta in un'azienda per esempio dovrebbe conoscere i rischi associati alle vulnerabilita' XSS.
*Step 2 non fidarsi di ogni input da parte di un user
Trattare tutti gli input degli user con diffidenza,tutti gli input di un user che sono usati come parte di un HTML output ci conducono ad un rischio di XSS.
*Step 3 usare escaping/encoding
Usare tecniche di escaping/encoding dipendentemente da dove gli input dell user arrivano: HTML escape, JavaScript escape, CSS escape, URL escape, etc.E' preferibile usare librerie gia' esistenti.
*Step 4 sanitizzare HTML
Se gli input dell user hanno il bidsogno di usare il linguaggio HTML,non si possono usare tecniche di eeescaping/encoding perche' andrebbero ad influire su comportamenti validi.In questo caso bisogna usare librerie certificate e sicure di HTML.Esempio HtmlSanitizer per.NET
*Step 5 settare HttpOnly flag
Per mitigare le consequenze di un possibile attacco XSS,settare HttpOnly flagper i cookies,in questo modo i cookies non saranno accessibili dalla parte client-side JavaScript.
*Step 6 usare una Content Security Policy
Per mitigare le consequenze di un attacco XSS si possono usare anche Content Security Policy (CSP).CSP e' un'intestazione della risposta Http che ti permette di dichiarare le risorse dinamiche alle quali e' concesso caricare dipendendo dall'origine della richiesta.
*Step 7 scansioni regolari
Scansionare regolarmente web applications con tool specifici.

SQL injection
Per prevenire un attacco sql injection ci sono diverse tecniche dipendenti dal tipo di vulnerabilita',nel datbase SQL e nel linguaggio di programmazione.
*Step 1 trainig e consapevolezza
*Step 2 non fidarsi di ogni input da parte di un user
*Step 3 usare whitelists e non blacklists
Non filtrare gli input basandosi su una blacklist,un attacco svolto in una certa maniera aggirerebbe questo sistema di difesa.Se possibile verificare e filtrare gli input usando solo una whitelist'
*Step 4 usare le ultime tecnologie
Per esempio in PHP usare PDO piuttosto che MySQLi.
*Step 5 usare meccanismi verificati
Evitare la programmazione autonoma della protezione SQLi,usando invece tecnologie con meccanismi di difesa dedicati che usino query parametrizzate o procedure di storing
*step 6 scansioni regolari
Scansionare regolarmente web applications con tool specifici

2)
*Danno economico causato=10.500€
*Per prevenire un attacco di ddos bisogna ridurre la superficie di attacco,quindi ci assicureremo che le nostre applicazioni o risorse non siano esposte a pote,protocolli o applicazioni dalle quali non ci aspettiamo comunicazioni.in alcuni casi si puo' fare cio ineserendo CDNS(Content Dstribution Networks) o Load Balancers e restringendo il traffico diretto di internet ad alcune parti dell'infrastruttura come un DB server.Bisogna inoltre usare FIREWALL con impostazioni valide nello specifico un WAF(Web Appliocation Firewall),saper riconoscere il traffico di rete analizzando i vari pacchetti,conoscere la capacita' del server e quanti dati possono transitare su questo.
*Le azioni per fermare un attacco di Ddos possono essere queste:bloccare IP attaccante,cambiare il proprio indirizzo IP/URL,spegnere Hardware,attivare protezioni ulteriori od ingaggiare service providers.

3)

Per evitare che l'attacco si propaghi nella rete interna andremo a rimuovere la macchina dalla nostra rete cambiandone L'indirizo IP,rimuovendo inoltre la macchina infetta dal FIREWALL creando regole nuove,in questo modo potremmo analizzare la macchina con calma senza correre il rischio che quest'ultima ne infetti altre.

REPORTS

1)Sembra essere un'attacco mirato all'utilizzo di una reverse power shell per ottenere informazioni e spazio di manovra,serve una scansione di rete patch ed esclusione dell'attacante e della macchina attaccata dalla rete.

2)Update malevolo da sovrascrivere usare FIREWAll che analizzino dati file (antivirus).