1. Le funzionalità di un Intrusion Detection System sono: l'analisi del traffico di rete, dei file di log ed in generale di tutti gli eventi interni al sistema che possono essere oggetto di attività illecite; il rilevamento di eventi anomali, quali intrusioni, attacchi o violazioni delle politiche di comportamento che si è deciso di adottare quando si opera sul sistema; tenere traccia di quanto rilevato grazie a database e file di log di diversa natura; permettere all'utente di visionare off-line un report di tutto ciò che è' stato rilevato come attività anomala o illecita.

2. Gli IDS presentano tre grandi problemi: sono sistemi la cui attività si limita generalmente al monitoraggio ed alla rilevazione di attività anomale, senza possibilità di contrastarle; non forniscono una visione della reale situazione del sistema poiché non hanno un'interfaccia di tipo real-time; non possono agire in modo autonomo, ma necessitano di una costante interazione con l'utente.

3. L'obiettivo che ci si è proposti è quello di rendere gli IDS uno strumento di difesa attiva in grado di riconoscere automaticamente il tipo di attività sospetta rilevata e le contromisure da adottare per contrastare al meglio gli effetti di tali attività. Si vuole inoltre fornire agli IDS un'interfaccia che permetta un'interazione real-time con l'utente fornendogli la situazione attuale del sistema. L'IDS così modificato prende il nome di Intelligent-IDS.

4. Si tratta di un Intrusion Detecion Sistem in grado di sfruttare le potenzialità di un sistema esperto per identificare gli attacchi e le attività anomale rilevate al fine di attivare, o comunque suggerire, le contromisure più efficaci da adottare.

5. Per creare l'Intelligent-IDS si è progettato e realizzato SLUNP utilizzando il sistema esperto CLIPS. Si tratta di un sistema adattativo che si connette con Prelude-IDS utilizzando un'interfaccia progettata ad hoc.

6. CLIPS è uno strumento per lo sviluppo e la distribuzione di sistemi esperti. Come tutti i sistemi esperti è in grado di utilizzare il paradigma di programmazione rule-based che sfrutta regole ed eventi per emulare la capacità di ragionamento umana. CLIPS è inoltre in grado di utilizzare il paradigma di programmazione procedurale e quello object-oriented. Presenta inoltre un alto grado di portabilità in quanto è stato sviluppato utilizzando il linguaggio di programmazione C++. Fornisce inoltre molti strumenti per la verifica e la validazione di sistemi esperti.

7. Prelude-IDS è un sistema di monitoraggio di reti ed host composto da uno o più manager, da più sensori di varia natura, da database e file di log e da un front-end che permette un'analisi dello storico degli eventi rilevati.

8. SLUNP è il sistema realizzato. E' il cuore dell'Intelligent-IDS: riconosce i vari allarmi generati da Prelude-IDS ed attiva, o suggerisce, le contromisure più adeguate. E' dotato di grande autonomia, ma in casi particolari può richiedere l'interazione con l'utente.

9. Durante la fase di progettazione, al fine di favorire l'aggiornamento di SLUNP, si è effettuata una classificazione degli attacchi ad oggi conosciuti in 23 tipologie distinte. Si sono progettati alberi decisionali specifici per ogni singola tipologia di attacco. La fase successiva ha visto la realizzazione del sistema base funzionante e l'implementazione degli alberi decisionali relativi ai sovraccarichi di sistema ed agli attacchi appartenenti alla tipologia PORT SCAN. Come ultimo passo si è realizzata l'interfaccia fra SLUNP e Prelude-IDS.

10. SLUNP richiede l'interazione con l'utente solo quando è strettamente necessario, fornendo tutte le informazioni in suo possesso relative all'allarme analizzato. All'utente può essere richiesta l'autorizzazione ad attivare contromisure particolarmente onerose oppure, se lo richiede, può essere lasciato libero di attivare manualmente le contromisure ritenute più opportune.

11. Quindi, come detto, SLUNP può agire in modo autonomo, richiedere la conferma all'utente su quanto deciso oppure lasciare libero l'utente di attivare manualmente le contromisure.

12. Per giungere ad una decisione, SLUNP utilizza sia dati iniziali, contenuti in un database interno chiamato "base delle conoscenze", sia alberi decisionali, come quello mostrato in questa slide. In particolare, questo è uno degli alberi decisionali relativi alla gestione di attacchi appartenenti alla tipologia port scan. Viene utilizzato da SLUNP dopo che l'Intelligent-IDS ha rilevato e contrastato il primo attacco appartenente a questa tipologia. SLUNP apre una finestra di attesa di X minuti all'interno della quale verifica che non vi siano ulteriori port scan. Se non ve ne sono, SLUNP non attiva ulteriori contromisure poiché ci si è trovati di fronte ad un evento isolato non significativo. Al contrario, se entro la finestra di attesa vengono rilevati nuovi port scan SLUNP deve attivare ulteriori contromisure. Si procede quindi all'analisi dell'indirizzo IP della sorgente dell'attacco. Se questo è spooffato, SLUNP necessita dell'interazione con l'utente poiché non è in grado di contrastare l'attacco in modo automatico. Qualora l'indirizzo IP non è spooffato e la sorgente dell'attacco è esterna alla rete locale a cui è connesso il sistema, SLUNP attiva contromisure specifiche, come l'invio di e-mail di avvertimento all'attaccante e l'introduzione di nuove regole ne firewall allo scopo di impedire all'attaccante di effettuare ulteriori connessioni per un determinato numero di ore. Se la sorgente è invece interna alla rete locale, viene attivato un livello decisionale successivo.

13. Passiamo a considerare come l'Intelligent-IDS realizzato sia in grado di rilevare e riconoscere un attacco della tipologia port scan. Innanzitutto viene attivato sull'host da proteggere Prelude-manager; viene poi attivato sullo stesso host il sensore Prelude-NIDS che effettua una connessione sicura con il manager. In una seconda macchia, che fungerà da attaccante, viene attivato un tool di esplorazione della rete per simulare un attacco port scan. Questo attacco viene rilevato da Prelude che attiva SLUNP il quale riconosce l'attacco ed agisce seguendo quanto previsto dall'albero decisionale implementato. Durante i test effettuati si sono rilevati tempi di reazione dell'ordine di 10 secondi; dove per tempo di reazione si intende il tempo trascorso da quando il manager riceve l'allarme del sensore sino alla richiesta di conferma dell'utente. Come mostrato dal grafico, l'80% del tempo di reazione viene impiegato per la visualizzazione a video del codice sorgente di SLUNP; si tratta di un vincolo di CLIPS che deve essere eliminato se si vuole aumentare l'efficacia dell'Intelligent-IDS.

14. Durante questa tesi si è effettuata una progettazione completa del sistema SLUNP, si è implementata parte degli alberi decisionali allo scopo di realizzare un sistema funzionante su cui si sono effettuati test di verifica e studi delle prestazioni.