STUDIO TECNICO DI INGEGNERIA INFORMATICA

ING. GIANLUCA GOLINELLI

Informatica Forense e Sicurezza Informatica

www.gianlucagolinelli.it – g.golinelli@gianlucagolinelli.it

Monitorare le reti mediante IDS Intrusion Detection Systems

(Durata: 8 h)

DOCENTE
Dott. Ing. Gianluca Golinelli

Ingegnere elettronico, membro del C3I (Comitato Italiano Ingegneria dell'Informazione), board member di A3I (Associazione Italiana Ingegneri dell'Informazione), Coordinatore del Gruppo di lavoro di Informatica dell'Ordine degli Ingegneri della Provincia di Parma. Si occupa da anni di sicurezza informatica come consulente per aziende ed enti della Pubblica Amministrazione, per cui ha svolto attività di formazione e consulenza. Svolge inoltre attività di informatica forense in qualità di Consulente Tecnico di Parte e Consulente Tecnico d'Ufficio del Tribunale di Parma.

Destinatari
IT Manager
Responsabile Sicurezza Informatica,
Tecnico di Sicurezza Informatica,
Consulenti Tecnici d'Ufficio,
Consulenti Tecnici di Parte

Obiettivi
Conoscere gli strumenti utilizzabili per monitorare la sicurezza della propria rete. Impostare opportune logiche di auditing per gli eventi critici di violazione della sicurezza. Ottimizzare l'utilizzo degli strumenti di rivelazione delle intrusioni per la propria rete. Conoscere le possibilità in termini di contromisure in circostanze di violazioni della sicurezza, impostabili automaticamente mediante gli IDS. Esercitarsi concretamente sulla configurazione e l'utilizzo di un potente sistema IDS.

Prerequisiti: conoscenze base di sistemi operativi e di networking; conosce di base sull'utilizzo di Antivirus e Firewall.

Perché utilizzare un IDS nella propria rete
- Ruolo e funzioni degli IDS nella sicurezza della rete
- Punti di forza e debolezze
- Dove e quando gli IDS devono essere usati
- Chi amministra gli IDS
- IDS vs. Firewall
- Insourcing vs. Outsourcing

Classificazione degli IDS
- Tipologie di Intrusion Detection Systems:
  - Network-Based
  - Host-Based
  - IDS Ibridi
  - IDS passivi e IDS attivi
  - Integrity monitors
  - Anomaly Based
  - Kernel monitors
  - Real-time vs. Pole for later

Architettura degli IDS
- Componenti di un sistema IDS
- Sensori
- Collettori
- Console di gestione
- Metatools

IDS basati su Rete (Network based IDS)
- Introduzione
- Architettura
- Sistema distribuito a nodi di rete
- Vantaggi/Svantaggi

CASE STUDY:
le principali vulnerabilità dei sistemi e possibili utilizzi degli IDS
Momento di riflessione riguardante i casi proposti dai partecipanti: verranno prese in considerazione le vulnerabilità principali solitamente riscontrate e le possibili contromisure da adottare mediante IDS

IDS basati su Host (Host based IDS)
- Introduzione
- Architettura
- Sistema distribuito basato su host
- Vantaggi/Svantaggi

Le Signature degli IDS e loro analisi
- Concetto di Signature
- Vulnerabilità comuni
- Signature di traffico normale
- Signature di traffico anomalo

IDS Open Source
- Snort, Aide, Tripwire
  - Architettura
  - Installazione
  - Configurazione
  - Logging

ESERCITAZIONE PRATICA: Installazione e Configurazione di Snort, Simulazione di un tentativo di attacco, Analisi dei log registrati.

Contromisure agli attacchi mediante gli IDS
- Monitoraggio del traffico
- Generazione di messaggi di allerta: tipologie di allertamento
- Impostazione di azioni basate su politiche di sicurezza
  - Forzare la disconnessione della sessione
  - Bloccare l'accesso alla rete alla sorgente dell'attacco
  - Bloccare tutti gli accessi alla rete

Cenni sugli IDS Commerciali (Funzionalità, vantaggi e svantaggi)

ESERCITAZIONE PRATICA:
- Installazione e Configurazione di OSSec,
- Simulazione di un tentativo di attacco,
- Analisi dei log registrati.

Gli IDS nella gestione degli attacchi: tuning dei sistemi
- Sistemi early-warning
- Procedure di escalation
- Politiche di sicurezza e procedure
- Definire l'ambito degli attacchi ed incidenti da gestire
- Definizione dei livelli di allarme degli IDS
- Le possibili fonti di risposta agli incidenti
- Integrazione di IDS e Firewall
- Sviluppare un'efficace capacità di risposta agli incidenti

Prospettive future, risorse
- Meta-IDS, NFAT tools, honeypots
- Siti informativi
- Documentazione sul web