Monitoraggio del traffico di Rete

Tradizionalmente l'analisi del traffico si divide in due grandi famiglie: l'analisi pacchetto-per-pacchetto, che è finalizzata alla risoluzione di problemi puntuali l'analisi per flusso, ovvero raggruppando assieme pacchetti omogenei, che permette invece di realizzare un monitoraggio permanente delle attività di rete.Scopo di questo corso è di illustrare i concetti e le metriche di base nell'analisi di rete, e di analizzare i protocolli e le metodologie più comuni di monitoraggio del traffico. Sono analizzati gli strumenti di monitoraggio del traffico più diffusi, e alcuni problemi reali e proposte soluzioni concrete. Alle sessioni di teoria, saranno affiancate esercitazioni pratiche sui concetti trattati.

Agenda (3 giorni)

Introduzione al monitoraggio del traffico di rete.

Metodologie di misurazione di rete: RFC 1242, RFC 2285, RFC 2432, RFC 1944, RFC 2544.

Metriche di base: throughput, latenza, pacchetti persi, jitter, throughput, disponibilità.

Misurazioni per link o end-to-end, inline o offline, attivo o passivo.

Introduzione a SNMP.

Monitoraggio di rete utilizzando SNMP: MIB II, bridge MIB, RMON, Cisco NBAR.

Monitoraggio orientato ai flussi: NetFlow, IPFIX e sFlow.

Analisi degli accessi di rete e misurazione del traffico utilizzando RADIUS.

Alcuni casi reali di monitoraggio di rete.

Cattura dei pacchetti di rete: problematiche, tap vs port span, tipologie di reti.

Librarie per la cattura del traffico di rete: libpcap e PF_RING.

Analisi del traffico basato su pacchetti: concetti di base (TCP/IP), analisi di protocolli comuni presenti in rete.

Memorizzazione e collezionamento dei dati di traffico: database SQL, raw files, RRD (Round Robin Database).

Geolocalizzazione degli host e delle comunicazioni di rete.

Utilizzo efficiente dei sistemi multi-core nell'ambito dell'analisi del traffico di rete.

La parte pratica

SNMP: Utilizzo del MIB-II per la realizzazione di semplici strumenti di monitoraggio di apparati.

NetFlow e sFlow: configurazione ed utilizzo sui più comuni apparati di rete (Juniper e Cisco), utilizzo di strumenti open source (ntop e nProbe) per la raccolta, visualizzazione ed analisi dei flussi di rete.

Memorizzazione di grandi moli di dati: DB relazionali vs DB bitmap.

Consolidamento di metriche di traffico nel tempo: RRD.

Analisi approfondita di Wireshark uno strumento avanzato per l'analisi di pacchetti di rete.

Implementazione di semplici programmi basati su libpcap per la cattura dei pacchetti di rete.

Obiettivi

A conclusione del corso i partecipanti saranno in grado di utilizzare i più comuni strumenti di monitoraggio di rete e di poter utilizzare al meglio i sistemi di analisi del traffico presenti in molti apparati di rete.

Destinatari e Prerequisiti

A chi è rivolto

Amministratori e tecnici di rete (End-User, Internet Service Provider, rivenditori di apparati e società di consulenza), responsabili e tecnici di Provisioning e Operation.

Prerequisiti

Conoscenze di base di informatica e di networking.

Iscrizione

Quota di Iscrizione: 1.690,00 € (+ IVA)

La quota comprende la didattica, la documentazione, il pranzo e i coffee break. Al termine del corso sarà rilasciato l'attestato di partecipazione.

Partecipazioni Multiple

Per le partecipazioni multiple che provengono da una stessa Azienda, è adottata la seguente politica di sconto:
10% sulla seconda
40% sulla terza
80% dalla quarta in poi.

Informazioni

Segreteria Corsi - Reiss Romoli s.r.l. - tel 0862 452401 - fax 0862 028308
corsi@ssgrr.com

Date e Sedi

Date da Definire

È un corso GOLD

con due partecipazioni potrai concordare con noi la data. Guarda i vantaggi della formula GOLD.

Formazione in House

Il corso può essere svolto presso la sede del Cliente e personalizzato nei contenuti.

Segreteria Corsi - Reiss Romoli s.r.l. - tel +39 0862 452401 - fax +39 0862 028308
email: corsi@ssgrr.com