Nuove attività del gruppo Security

Rimini, 11 Maggio 2007

Pistolotto

- Molta (troppa?) carne al fuoco
  - topologia LAN
  - servizi essenziali
  - token USB
  - auditing
  - documentazione Harmony
- Necessario coordinare il lavoro con gli altri gruppi, in particolare il netgroup
- Nuove adesioni più che benvenute!

Topologia LAN

- Configurazioni ottimali rete e monitoraggio, ai fini della minimizzazione dei rischi e danni in caso di intrusione.
- **Carbone**, Alfieri, Belluomo, Covati

Topologia LAN: attività prevista 1/2

- Analisi della situazione “media” in termini di servizi erogati e rischi connessi;
- individuazione di alcune topologie standard da fornire “chiavi in mano” alle sedi;
- proposte di implementazione reale delle topologie via soluzioni possibilmente **non proprietarie;**

Topologia LAN: attività prevista 2/2

- formulazione di una lista di porte da filtrare e/o di regole di massima per la “saggia ed efficiente” suddivisione del traffico (buona anche per chi abbia già implementato una particolare soluzione);
- definizione di una soluzione standard per
  - controllo/logging dell'attività di rete e della presenza di macchine e servizi a rischio
  - segnalazione tempestiva di potenziali pericoli (analisi traffico, active probes con nessus o simili, BOT discovery, etc.).

Servizi essenziali

- Configurazioni standard per alcuni servizi strategici, per fornire, e mantenere, distribuzioni di macchine virtuali
  - dns
  - log server (tool analisi log)
  - integrity checker (samhain)
  - servizi windows (?)
  - intrusion detection (argus, snort, ntop)
  - ...
- Costa, Donatelli, Veraldi

Token USB

- Scelta del modello più adatto per la nostra realtà
  - compatibilità windows / linux
  - capienza
- Due tipi di certificati
  - per firma (generati nel token)
  - per cifratura (importati nel token)
- **Veraldi**, Casale, Cecchini

Utilizzo token 1/2

- Accesso wireless
  - certificati per 802.1x utilizzabili anche da Windows
- VPN
  - accesso solo con certificati?
- Accesso web
- Grid
  - ad es.: http://doiop.com/nikhef_token
- Cifratura e firma digitale

Utilizzo token 2/2

- Single Sign On
  - Cosign
  - CAS
  - WebAuth
  - A-Select
  - Kerberos (RFC 4556)
  - OpenID
- Procedure gestionali
  - “ufficializzazione” validità certificati INFN CA

Auditing

- Meccanismo per la verifica della sicurezza delle varie reti locali
  - scansioni da remoto (per ora...)
    - tre – quattro server
    - nmap, nessus, sara, nikto
- Brasolin, Cecchini, Michelotto

Documentazione Harmony

- Aggiornamento dei documenti accompagnatori del Regolamento d'uso delle risorse informatiche
  - wireless (**Brasolin**, Belluomo, Veraldi)
  - windows
  - mac (**Gianoli**)
  - firewall & router (netgroup?)