Tecniche di attacco informatico Perché hanno successo.

Paolo Santiangeli

Tipologie di Attacco

- Sfruttamento di cattive configurazioni
- Sfruttamento di vulnerabilità (exploits)
- Bruteforce Attacks e Password Guessing
- *Sniffing*
- *Identity Spoofing*
- *IP Hijacking (vedente e cieco)*
- *Denial Of Service*
- Social Engineering
- Etc.

Fattore Umano (Human Threat)

“Meno del 40% degli attacchi avviene dall’esterno.”

- Password semplici e/o facilmente intuibili
- Implementazione tardiva delle patch

Dove il fattore umano è preponderante

- **Sfruttamento di cattive configurazioni**
- **Sfruttamento di vulnerabilità (exploits)**
- **Bruteforce Attacks e Password Guessing**
- **Social Engineering**

Human Threat Risk Mitigation

- Password Enforcement
- Patch Management
- User Training

Password Enforcement

- Password di lunghezza inferiore agli 8 caratteri e cambiate almeno ogni 30 giorni
- Password non facilmente intuibile
- Password diversa per ogni utente

Suggerimenti per le Password

Criteri di codifica personali

- L’acronimo di un verso poetico, una massima o una frase
- Uso di lettere e numeri
- Dispari maiuscola - pari minuscola

Un esempio

- O Luce Etterna Che Sola In Te Sidi:
  OLECSITS
- Sostituire 1 e 0 alle lettere i e o
  0LECS1TS
- Dispari maiuscola - pari minuscola
  0lEcS1Ts

Patch Management

- L’applicazione delle patch software non è implementata o risulta essere tardiva
- La maggioranza dei virus, dei worm che usano exploit avrebbero avuto un effetto ridotto se le patch fossero state implementate appena uscite

Patch Management Tools

Workstation

- windowsupdate.microsoft.com
- officeupdate.microsoft.com

LAN

- Microsoft Sistem Update Services
  [http://www.microsoft.com/windowsserversystem/sus/default.mspx]
- Microsoft Baseline Security Analizer
  [http://www.microsoft.com/technet/security/tools/mbsahome.mspx]

INFO

- Open Vulnerability Assessment Language
  [http://oval.mitre.org/index.html]

Social enginering

Definizione

L’arte di portare una persona a rivelare informazioni e dati sensibili riguardanti i sistemi da essa usati anche tramite lo stimolo di azioni opportunamente sollecitate, come ad esempio l’attivazione di un attachment di una email

Sensibilizzazione

Sensibilizzazione del personale

- Alla sicurezza ed alla privacy delle informazioni aziendali
- All’uso di Internet e dei rischi ad esso connessi dialer, cavalli di troia e spyware

Training

Formazione del personale

- L’implementazione della protezione contro i virus, i firewall, ed le tecnologie di content filtering possono aiutare a controllare i fattori di rischio.
- Il comportamento di un utente può compromettere la sicurezza della rete
- La formazione degli utenti è una misura chiave per la strategia della sicurezza della rete