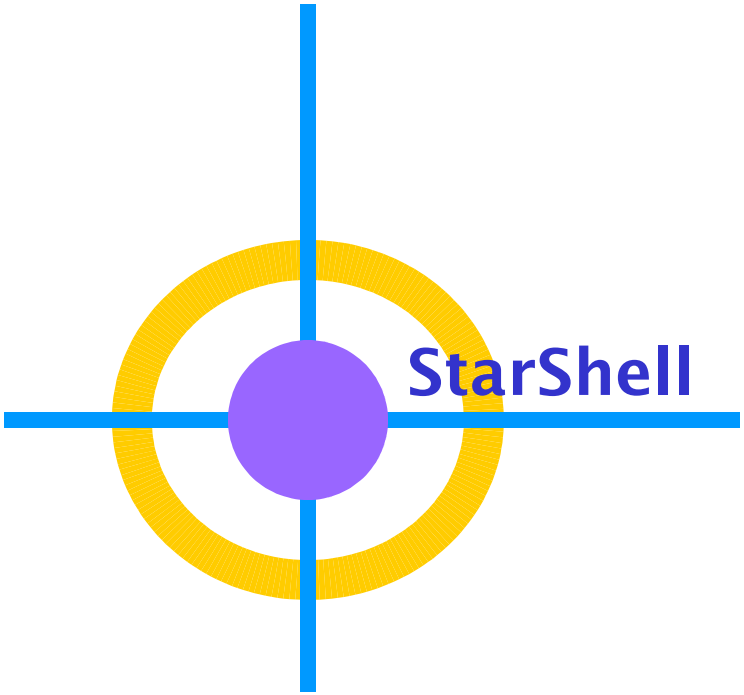


Il Lato Oscuro

Attacchi

- **Confidenzialità**
  - Da Segretezza a Privacy
- **Integrità**
  - Autorevolezza (risvolto: Non Ripudiabilità)
- **Disponibilità**
  - Diniego di Servizio

Modello **CIA**

(Confidentiality, Integrity, Availability)

Figure Attive (Attaccanti)

- Tipi:
  - Alti Ideali
    - **Servizi Segreti/Nazionali (*Cyberwarfare*)**
    - **Terroristi e Nemici**
  - Lucro
    - **Mafie e Spionaggio Industriale**
    - ***Criminali Privati***
  - Psicologia Perversa
    - ***Vendicatori***
    - ***Hackers***

  Collettivi: Servizi Segreti/Nazionali (*Cyberwarfare*), Terroristi e Nemici, Mafie e Spionaggio Industriale, *Criminali Privati*

  Individui: *Criminali Privati*, *Vendicatori*, *Hackers*

- Operazioni aperte o coperte

Servizi Segreti e Terroristi

  - Scopo: alti ideali
    - **patria, libertà, religione**
  - Principalmente raccolta informazioni
  - Operazioni coperte con preparazione ad attacchi coperti o scoperti
  - Non ci si può validamente difendere
  - Le difese attive possono causare ritorsioni
  - Incidenza relativamente rara
- Cyberwarfare
  - Offensive
  - Defensive
  - Preventive offense

Mafie e Spionaggio Industriale

- Scopo: lucro
- Operazioni coperte
- Raccolta informazioni riservate
- Modifica archivi
- Diniego di servizio parziale o totale
  - **Vantaggio differenziale per la concorrenza**
- Mezzi informatici a volte potenti
- Uso di basisti interni

Criminali

- Scopo: lucro personale
- Operazioni coperte
  - **non vogliono danneggiare il nostro sistema**
- Operazioni continuate
  - **Tecniche di 'salami slicing'**
- Operazioni 'una tantum'
  - **modifiche archivi (conti correnti, voti esame, ecc.)**
- Principali sospetti: personale interno, consulenti

Vendicatori

- Scopo: ritorsione o sabotaggio
  - **iniziativa personale**
  - **vendetta di torti subiti**
  - **copertura illeciti**
  - **diversivi: attacchi ad altri sistemi**
- Attacchi di Diniego di Servizio
- Sospettati principali:
  - **amministratori di sistema e di reti**
  - **ex dipendenti o consulenti**
  - **personale interno per evitare lavoro**

Hackers

- Scopo 1: bravata personale
  - **esibizione nei confronti dei pari**
  - **acquisizione conoscenze e competenze**
- Scopo 2: utilizzo sistemi
  - **per archivi o programmi illegali**
  - **come base di attacco ad altri sistemi**
- Importante studiare la ‘filosofia’ Cyberpunk
  - **William Gibson e Bruce Sterling**
  - **anarchia e nichilismo**

Si possono tollerare gli Hackers?

- Metodi di attacco nuovi e raffinati
  - **Si può imparare molto da loro**
  - **Evidenziano debolezze da correggere**
- Scopi non intenzionalmente malvagi, ma:
  - **Indeboliscono le difese nei confronti di altri attaccanti**
  - **Pubblicizzano debolezze, password, ecc.**
  - **A volte sbagliano e danneggiano**

“Ma non ho niente da difendere”

- E’ proprio vero?
  - **adesso**
  - **in futuro**
  - **con altri sistemi**
- Responsabilità legali nei confronti di:
  - **utenti locali dei sistemi**
  - **altri sistemi di altre aziende ed enti**
- Una volta entrati gli Hackers ritornano
  - **difficili da estirpare**

Impiegare Hackers per la difesa

- Mito: “Ci vuole un ladro per acchiapparne un altro”
- Psicologia bacata:
  - **sono veramente leali all’azienda?**
  - **“non ci indurre in tentazione”**
- Job Turnover
  - **avranno I nostri segreti anche nel prossimo loro lavoro**
  - **possono impiantare ‘back-doors’ e bombe logiche o a tempo**

- Fasi evolutive:
  - 1. Impiegare gli hacker per la difesa
  - 2. Tolleranza zero
  - 3. Impiegare hacker per spionaggio industriale e 'intelligence competitiva'

Tipi di Hacker

- **Novizio** *(Script Kiddy, Lamer)*
  - Si vanta molto, prova attacchi semplici, viene preso subito
- **Studente**
  - Nega di essere uno hacker, consulta siti sullo hacking, crittografa i file, legge libri, studia il linguaggio C
- **Studioso**
  - Ha cambiato luogo, nessuno lo sospetta; opera da altri computer, usa metodi steganografici, usa molti sistemi operativi, ha possibilità economiche
- **Guru**
  - Noto nel settore, è un ottimo programmatore; non è più uno hacker attivo, ha perso l'onda; ha punti di vista filosofici, forse scrive un libro.

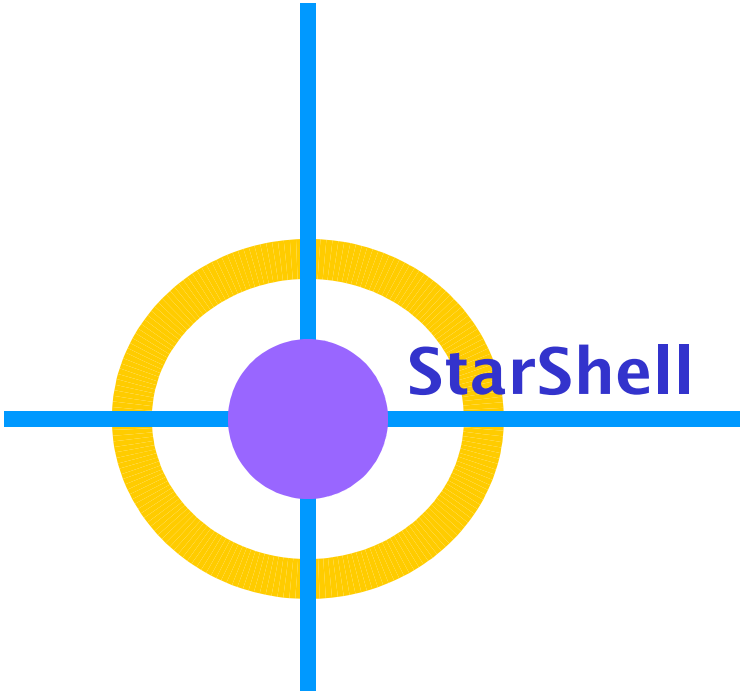
Attaccanti di Elite

- Compiono attività che:
  - Non vengono di solito osservate
    - **ICMP, SMTP, POP, NNTP**
  - Sono difficili da scoprire
    - **Canali coperti**
  - Sono difficili da ripetere
    - **X Windows, NetBus, encrypted**
  - Rendono difficile rintracciare l'IP del mittente
    - **DoS, Relay di posta, anonimizzatori**
  - Rendono difficile la raccolta di prove
    - **Steganografia, crittografia, trappole**
  - Mantenere diniego plausibile
    - **Login rubati, connessioni internet pubbliche**

Prendiamo solo i più gonzi

Minacce Interne

  - National Security Information Exchange (NSIE – 1998)
- Impiegati insoddisfatti
- Spie prezzolate
- Impiegati ricattati o compromessi
- Ex-impiegati
- Pseudo-impiegati
  - Consulenti, A tempo parziale, A contratto, Vigilanti
- Soci in affari


StarShell