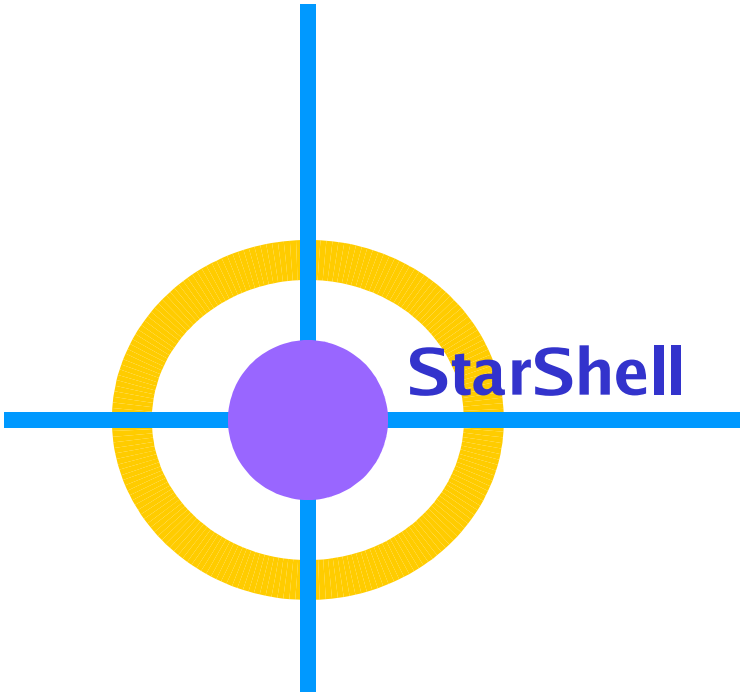


Le 10 Principali Vulnerabilità in Rete

Vulnerabilità più Critiche

- Non sono tutte le vulnerabilità esistenti
- Cambiano come la moda
- Sono le più sfruttate al momento
- Per sistemi in rete attaccati dall'esterno

- Concentrarsi prima sulle vulnerabilità critiche
- Poi affrontare le altre vulnerabilità

1 - BIND

- Berkeley Internet Name Domain
  - Software implementativo del servizio DNS
  - Versioni vecchie (4.x) sono molto vulnerabili
  - Tutte le versioni attaccate con ‘Buffer Overflow’
  - Vengono consentiti i ‘Zone Transfer’ indiscriminati
  - I responsi non prevedono autenticazione
- Difese
  - Aggiornare il software
  - Proibire i ‘Zone Transfer’ fuori dominio
  - Isolare il server DNS da altri servers

2 - Script CGI

- Common Gateway Interface
  - Programmi per generazione pagine dinamiche
  - Scritti in Perl, Shell o linguaggi compilati

  - L'uso di linguaggi interpretati è pericoloso
  - Alcuni esempi forniti col Server Web sono bacati

- Difese
  - Rimuovere gli esempi di default
  - Usare ultime versioni di Perl
  - Preferire linguaggi compilati e sicuri (es. Java)

3 - RPC

- Remote Procedure Call
  - Strato di sessione per molti applicativi di rete (es. NFS)
  - Non fornisce validazione
  - Soggetto a ‘spoofing’ ed intercettazione
  - Versioni vecchie più vulnerabili

- Difese
  - Disabilitare RPC ed i suoi servizi se possibile
  - Installare l’ultima versione e le ‘patch’
  - Usare RPC Sicuro (Kerberos) se possibile
  - Crittografare il canale di comunicazione (SKIP, PPTP)

4 - MS IIS

- Microsoft Internet Information Server
  - Web Server di Windows NT/2000
  - Componente RDS (Remote Data Services) è molto vulnerabile a buffer overflow
  - Esecuzione comandi, variazione configurazione
  - La tecnologia COM/ActiveX può facilmente inviare virus

- Difese
  - Applicare patch Microsoft
  - Non utilizzare IIS, sostituire con, p.es. Apache
  - Usare Java invece di COM/DCOM

5 - Sendmail

- Protocollo SMTP su piattaforme UNIX
  - Programma grosso e con molti bachi storici
  - File di configurazione molto complesso
  - Permette spesso acquisizione di informazioni indebita
  - Soggetto ad attacchi di buffer overflow

- Difese
  - Usare ultime versioni ed applicare ‘patch’
  - Ridurre al minimo il file di configurazione
  - Usare solo entro un Firewall
  - Sostituire con altre utilities (qmail, Postfix)

6 - sadmind, mountd

- SW di amministrazione o montaggio FS da remoto
  - Tutti i programmi di amministrazione remota sono pericolosi (anche in Linux ed NT)
  - mountd da il primo ‘handle’ ad un file system remoto
  - Mancano di autenticazione
  - Vulnerabili a buffer overflow
  - Usati nei DDOS a Yahoo, ecc. nel 2000
- Difese
  - Ultime ‘patch’
  - RPC Sicuro (Kerberos) se possibile
  - Canale di comunicazione crittografato
  - Solo amministrazione locale o via SSH

7 - File Sharing

- Condivisione files e directories in rete
  - Bachi intrinseci del NFS o Network Neighbourhood
  - NFS: collisione potenziale di identificativi utente
    - **Soluzione richiede NIS, molto pericoloso a sua volta**
  - Win32: i default sono read-write per tutti
    - **Scarsa educazione degli utenti Windows**
- Difese:
  - Configurare appropriatamente NFS
  - Usare RPC/NFS Sicuro o canale crittografato
  - Usare Domini NT
  - Non usare Windows fuori dal Firewall

8 - Passwords

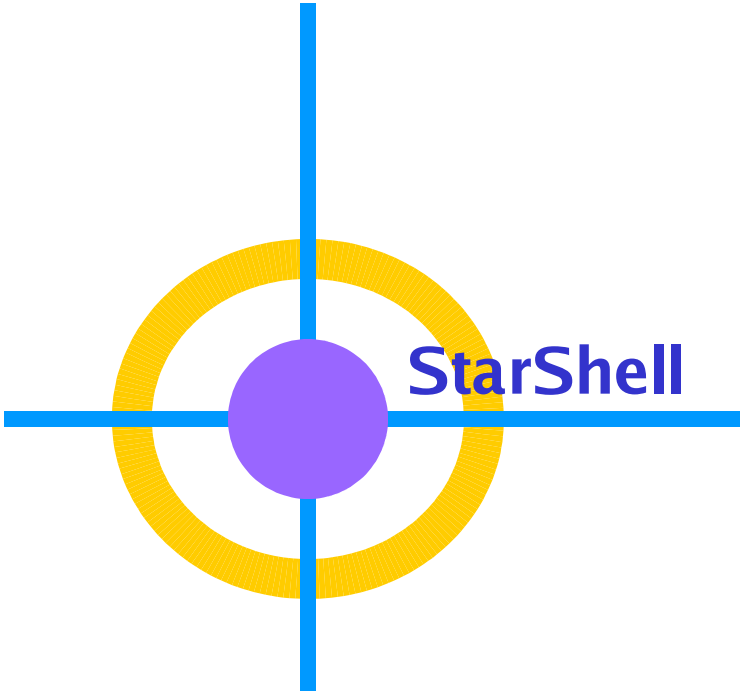
- Schemi di identificazione e autenticazione
  - Password assenti completamente
  - Password ‘di servizio’ note
    - **root/root, system/manager, scott/tiger, sanfran/cisco**
  - Password facilmente indovinabili
    - **‘password’, ‘pippo’, nomi di famiglia, iniziali, targhe**
  - Scritte sul video o nel cassetto
  - Cambiamento delle password
  - In files leggibili e asportabili
- Difese
  - Attacco preventivo di Cracking al proprio sistema
  - Educazione degli utenti e sanzioni amministrative

9 - POP e IMAP

- Post Office Protocol, Internet Mail Access Protocol
  - Protocolli di accesso a posta elettronica in arrivo
  - Programmi bacati e obsoleti
  - Mancanza di limitazioni di accesso
  - Password in chiaro sulla rete
    - **soggetti a 'sniffers'**
- Difese
  - Applicare ultime 'patch'
  - Usare solo entro Firewall
  - Usare versioni con autenticazione Challenge/Response
  - Usare canali crittografati
  - Crittografare la posta elettronica inviata

10 - SNMP

- Simple Network Monitoring Protocol
  - Sistemi di amministrazione distribuita e segnalazione di anomalie
  - La community di default è indovinabile
  - Non vi è certificazione intrinseca
- Difese
  - Configurare community alternative
  - Usare come parte di applicativi che inseriscono una certificazione
  - Impostare canali crittografati


StarShell