Università degli Studi di Salerno

Dipartimento di Informatica

Penetration Testing & Ethical Hacking

Postexploitation (Maintaining Access)

Parte 1

Arcangelo Castiglione
arcastiglione@unisa.it

Outline

- Concetti Preliminari
- Operating System Backdoor
- Web Backdoor

Outline

- **Concetti Preliminari**
- Operating System Backdoor
- Web Backdoor

Concetti Preliminari

- Dopo aver effettuato il *Privilege Escalation* sulla macchina target potrebbe essere richiesto di creare o installare meccanismi che consentano di mantenere l'**accesso persistente** ad essa
  - **Accesso Persistente:** poter accedere alla macchina target dopo che la vulnerabilità per accedervi è stata risolta o la macchina è stata riavviata

- **N.B.** Così facendo, anche se in futuro la vulnerabilità sfruttata per accedere alla macchina target verrà risolta, si potrà avere lo stesso accesso ad essa

Concetti Preliminari

- L'utilizzo di meccanismi di persistenza deve sempre essere reso noto e chiarito durante la fase di Target Scoping tra tutte le parti coinvolte nel processo di penetration testing

- È sempre necessario documentare tutti i meccanismi di accesso persistente installati durante la fase di Postexploitation
  - Così che tali meccanismi possano poi essere subito rimossi al termine del processo di penetration testing

Concetti Preliminari

- Le Regole di Ingaggio definite nella fase di Target Scoping a monte di un processo di penetration testing tipicamente non consentono esplicitamente di effettuare tale attività

- È necessario assicurarsi che l'**utilizzo di meccanismi di persistenza (ad esempio, backdoor)** sia stato **esplicitamente richiesto e consentito per iscritto**
  - Durante la fase di *Target Scoping* ed in particolare nella *Definizione delle Regole di Ingaggio*

Concetti Preliminari

- Gli strumenti per mantenere l'accesso persistente ad una macchina target sono generalmente classificati in tre categorie principali
  - Operating System Backdoor
  - Web Backdoor
  - Strumenti di Tunneling