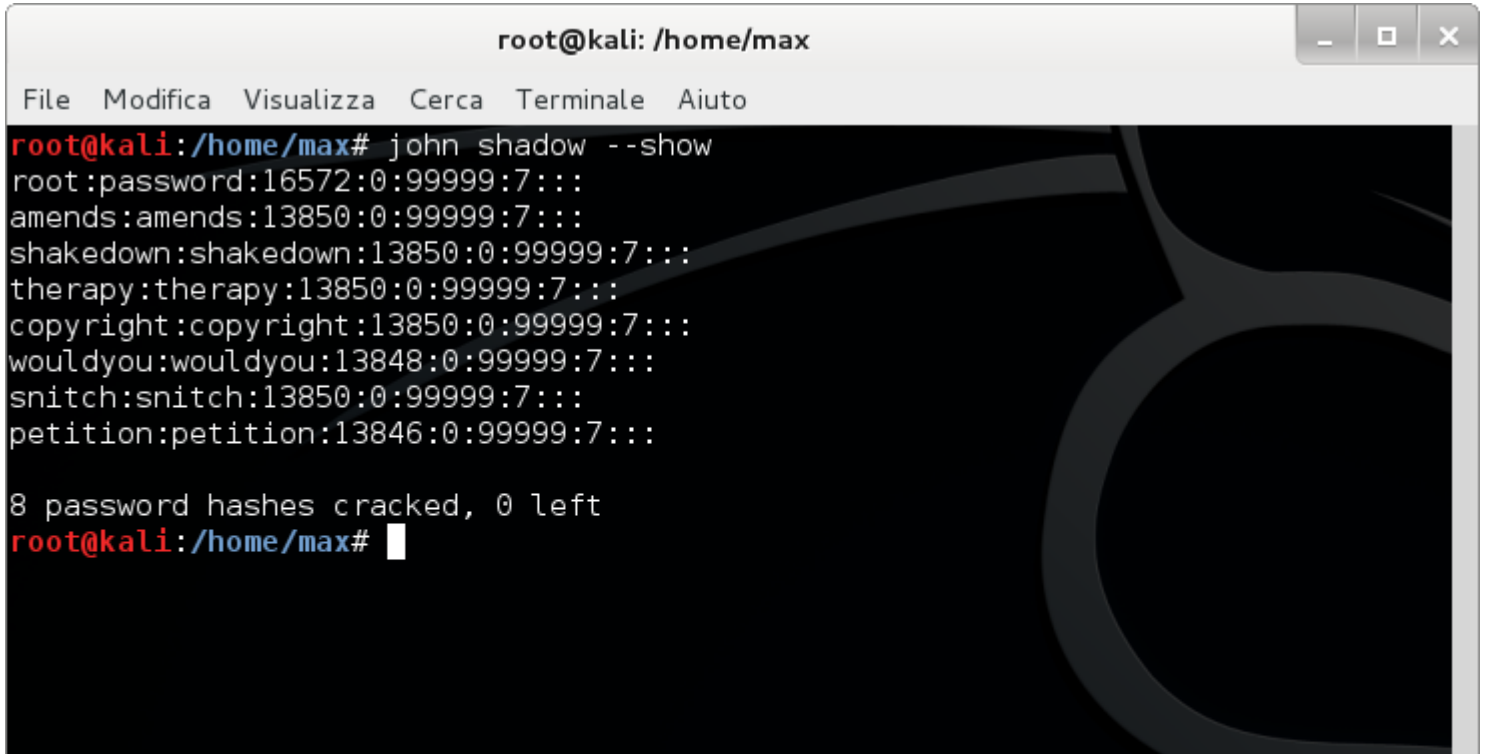
Attacco autenticazione Unix

- Estrazione file delle password */etc/shadow* dalla propria macchina vittima
- Password cracking con *John the Ripper* (attacco a dizionario di default)



Patch autenticazione Unix

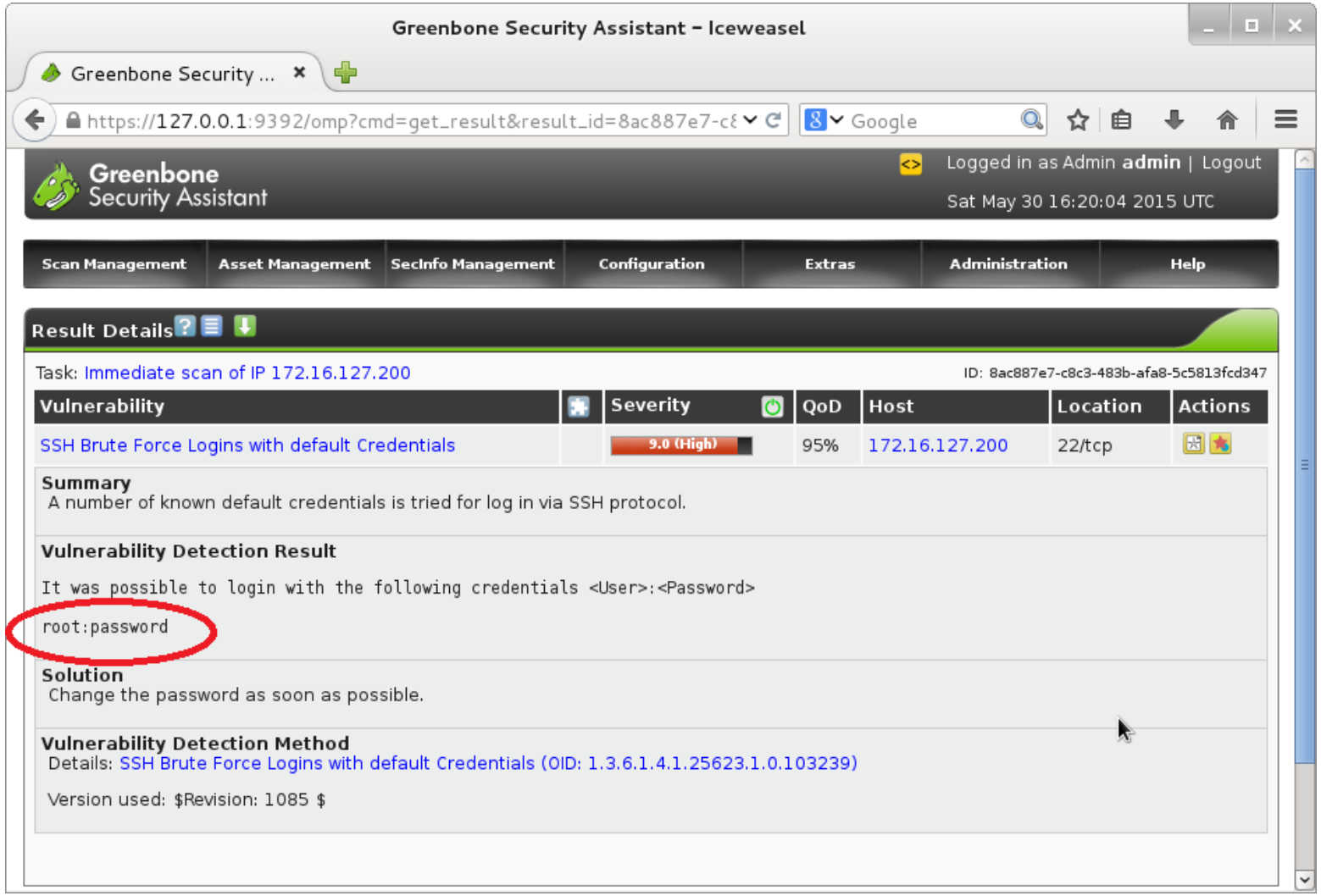
Preparazione fix:

- Password modificate nella nostra macchina vittima
- Inserimento nuovo file *shadow* nel «pacchetto di patch difensive»

Applicazione fix durante gara:

- Deploy del «pacchetto di patch difensive»
- Chiusura servizio SSH nella nostra vittima

OpenVAS SSH Brute Force

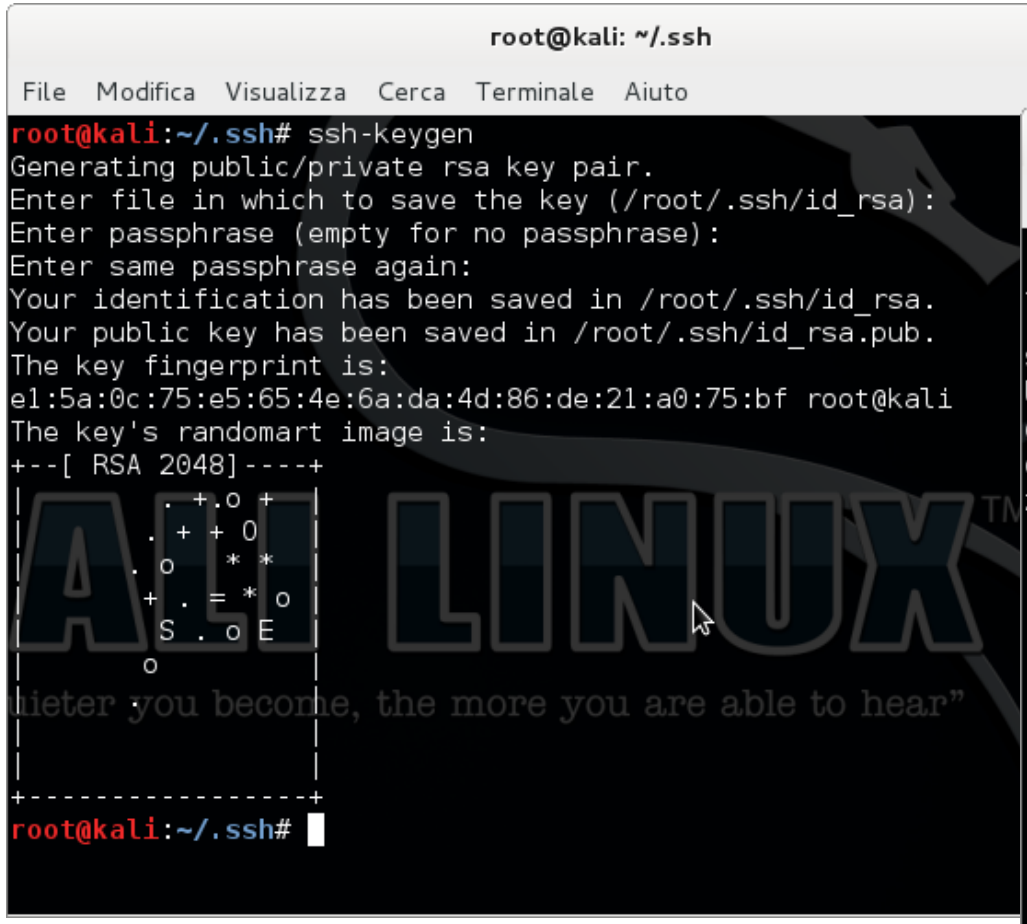


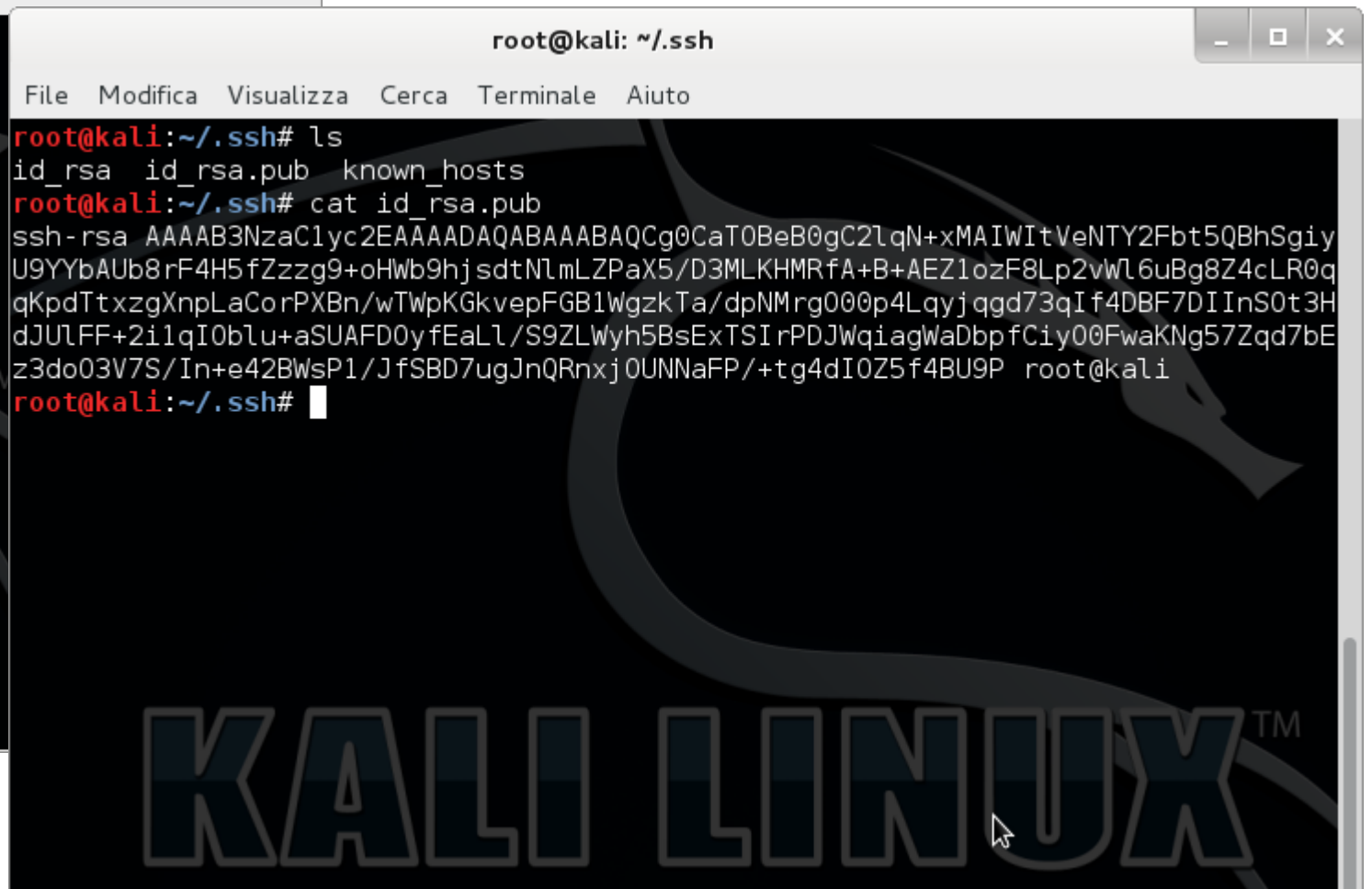
SSH autenticazione tramite chiavi RSA

- Autenticazione senza bisogno di password mediante chiave pubblica (server) e chiave privata (client)

- Utile se gli avversari cambiano le password o rimuovono la nostra backdoor

Generazione chiavi RSA





Caricamento chiave pub. su vittima

- Script *run_interactively* lancia shell sulla vittima
- Scrittura chiave pubblica su */root/.ssh/authorized_keys*