**ejpt**

sqlmap:

sqlmap –u url

🡪sqlmap –u url –tables

🡪sqlmap –u url –D namedatabase –T nametable –dump

Unshadow password hash >crakhash

🡪الاداه تعمل ع جمع الاسم مع الهاش الخاص به

John –wordlist<path wordlist> name hash file

Smbclient [\\\\ip\\path](file:///\\\\ip\\path) file open –N🡺للدخول الى الملف المفتوح بعد استعمال enum4linux

بعد ما فتنا اذا بدنا نوخذ ملف

Get filename /path where save

Run autoroute –s ipadres victim –n 255.255.255.0 (net mask)🡺للدخول من الضحيه الاولى للضحيه الثانيه

Portfwd add –l 1122 –p open port –r ip victim

وظيفتها تحول الاتصال من بورت 21 للبورت 1122 في جهاز المخترق

يتم عملها في الميتر بريتر

Nmap –sS –sV 1122 localhost 🡺يتم عملها في الميتا سبولويت

Searchexploit name exploit