1. **Kad presretnemo komunikaciju Internetskog preglednika i web poslužitelja, moguće je mijenjati i zaglavlje (header) paketa**Tocno
2. **Cod povezivanja exploit i payload komponenti u metasploit framework alatu, komponenta koja nakon provale u ranjivu aplikaciju/servis odradi ono što napadač želi nazivati**Payload
3. **Kako se naziva set alata (toolbox) koji smo koristili kod BoF ranjivosti za provalu na računalo i dobivanje shell-a?**Metasploit
4. **Napadac je iskoristio ranjivost u sustavu i dobio shell. Na shell se spojio pseudo naredbom spajamse na IP i port. Kako se naziva taj shell? Odaberi od navedenog:**Bind shell
5. **Sto ne valja sa sljedećim komandama metasploit framework-a (Uparite točne komande)?:
set exploit/windows/http/easyfilesharing post
use PAYLOAD windows/meterpreter/reverse\_tcp**Kod odabira payload-a moramo koristiti Use exploit
Kod odabira exploit-a moramo koristiti Set payload
6. **Kod napada na web aplikacije, promjenom parametara na klijentskoj strani možemo utjecati na izvršavanje poslužiteljskog koda. To se naziva parameter tampering. Navedite bar jedan alat kojim je to moguće raditi NAKON Što je paket napustio Internetski preglednik.**Burb