A black background with red text

Description automatically generated

***IT381 Zaštita i bezbednost informacija***

***Domaći zadatak br. 8***

***Ime i prezime: Jovan Pavkovic***

***Broj indeksa: 4442***

**Tekst Zadataka**

Za rešenje zadatka potrebno je:

1. Metasploit
2. Metasploitable 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 exploit.

Zatim pokrenite redom komande: „use exploit/multi/samba/usermap\_script“,

„set rhost ip\_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?

A screenshot of a computer

Description automatically generated**Rešenje zadataka**

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

Metasploit je moćan i široko korišćen okvir (framework) za testiranje penetracije, razvijen za potrebe sigurnosnih profesionalaca, istraživača i etičkih hakera. Kreiran je kako bi pružio alate za izvođenje testova penetracije, razvijanje sigurnosnih alata i simuliranje napada kako bi se identifikovale i ojačale bezbednosne slabosti u sistemima.

Evo nekoliko ključnih karakteristika i mogućnosti Metasploita:

**Modularnost**: Metasploit je modularan, što znači da koristi modularni pristup. Različiti moduli pružaju funkcionalnosti za različite zadatke, uključujući isporuku eksploatacija, skeniranje ranjivosti, postavljanje payloada, snimanje saobraćaja, itd.

**Payloads**: Omogućava korisnicima da ugrade "payloads" u ciljane sisteme nakon uspešnog eksploatacionog napada. Payloadi su komadići koda koji omogućavaju daljinski pristup i kontrolu nad sistemom, često korišćeni u svrhu testiranja sigurnosti.

**Eksploatacije**: Metasploit uključuje brojne eksploatacije koje se mogu koristiti za iskorišćavanje ranjivosti u ciljanim sistemima. Ovi moduli pomažu testiranje bezbednosti sistema kako bi se identifikovale slabosti.

**Automatizacija**: Metasploit podržava automatizaciju testova penetracije kroz skripte i automatizovane eksploatacije. Ovo je korisno za smanjenje vremena testiranja i povećanje efikasnosti.

**Post-exploitation moduli**: Omogućava analizu i eksploataciju ciljanog sistema nakon uspešnog eksploatacionog napada, uključujući prikupljanje informacija, postavljanje rootkitova, itd.

**Podrška za različite platforme**: Metasploit je dizajniran za rad na različitim platformama, uključujući Windows, Linux i macOS. Takođe podržava različite arhitekture.

**Zajednica i zajednička baza podataka**: Metasploit ima veliku i aktivnu zajednicu korisnika koji doprinose razvoju novih modula, exploit-a i tehnika.

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

Metasploit Framework (MSF) ima veliki broj komandi koje pružaju različite funkcionalnosti za testiranje penetracije. Evo nekoliko klasičnih i često korišćenih komandi unutar Metasploit Framework-a, zajedno sa njihovom namenom:

**msfconsole**: Ova komanda pokreće Metasploit konzolu, centralno mesto za interakciju sa svim Metasploit modulima i funkcijama.

**db\_status**: Proverava status povezane baze podataka. MSF koristi bazu podataka za skladištenje informacija o ciljevima, ranjivostima i eksploatacijama.

**use [modul]**: Omogućava odabir određenog modula. Na primer, use exploit/windows/smb/ms08\_067\_netapi biranje modula za eksploataciju ranjivosti MS08-067 u Windows SMB protokolu.

**show options**: Prikazuje opcije koje se mogu konfigurisati za odabrani modul. Nakon biranja modula, korisnik mora postaviti određene parametre, a ova komanda prikazuje dostupne opcije.

**set [opcija] [vrednost]**: Postavlja vrednost određene opcije. Koristi se nakon use komande kako bi se postavile vrednosti parametara za odabrani modul.

**exploit ili run**: Pokreće eksploataciju ili napad na ciljni sistem. Ovo je poslednja komanda koja se izvršava nakon postavljanja opcija.

**sessions**: Prikazuje aktivne sesije koje su uspostavljene sa ciljnim sistemima. Ako je eksploatacija uspešna, možete videti aktivne sesije.

**sessions -i [ID]**: Ulazak u određenu sesiju. Ako imate više aktivnih sesija, ova komanda omogućava prelazak u određenu sesiju koristeći njen ID.

**search [izraz]**: Pretražuje bazu podataka Metasploita za module koji odgovaraju zadatom izrazu.

**exit ili quit**: Izlazi iz Metasploit konzole.

1. **Ukratko opišite „username map script“ exploit.**

Ovaj modul koristi ranjivost u izvršavanju komande u Samba verziji 3.0.20 do 3.0.25rc3 kada se koristi ,,username map script,, konfiguraciona opcija. Ukoliko username sadrži posebne shell znakove moguće je izvršiti arbitrarnu komandu. Nike potrebna autentifikacija kako bi se ova ranjivost iskoristila.

1. **Šta vam je omogućio ovaj exploit?**

SQL injection, CMD izvršavanje, RFI i LFI.