Jesenji semestar, 2022/23

PREDMET: IT381 - Zaštita i bezbednost informacija

Domaći Zadatak br. 8

Student: **Aleksa Cekić 4173**

Profesor: **dr Milena Bogdanović**

Asistent: **mr Goran Stamenović**

Datum izrade: **19.03.2023**

Tekst Zadataka

Za rešenje zadatka potrebno je:

1. Metasploit
2. Metasploitable

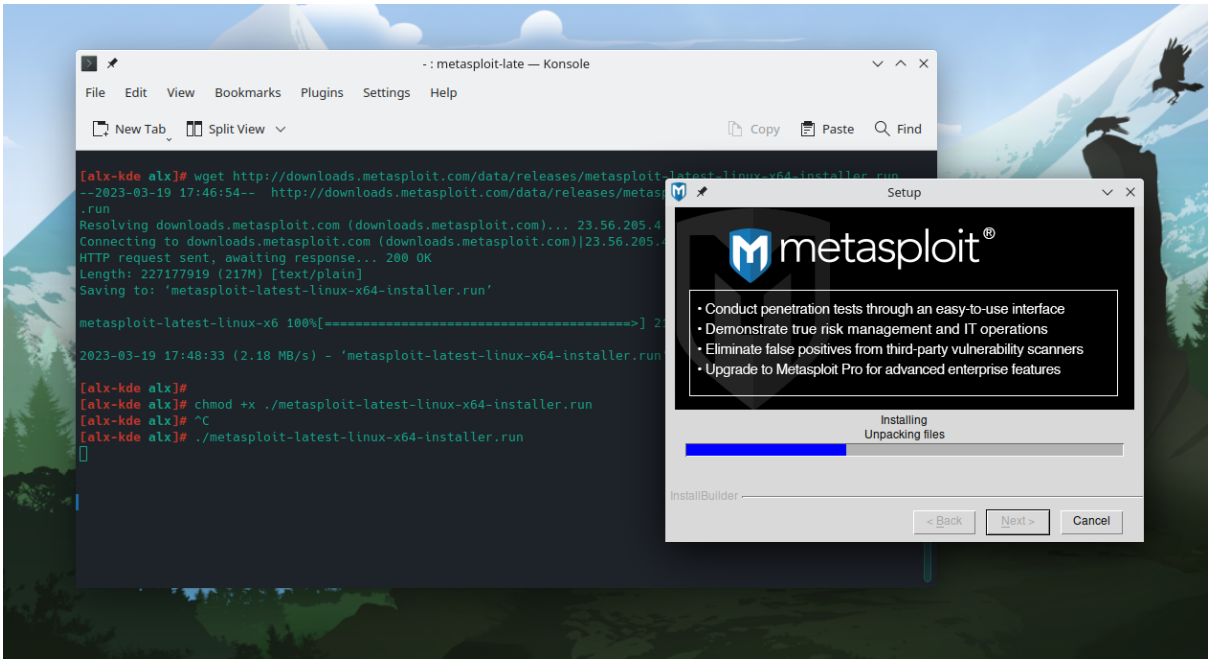
Zadatak

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?

Rešenje zadataka



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

Metasploit je bezbednosni projekat koji obezbeđuje informacije o bezbednosti i ranjivostima i pomaže kod testiranja penetracije sistema i izradu IDS potpisa. Njegove mogućnosti su NMAP skeniranja računara u mreži kao i pronalaženje exploita.

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

Komandom ifconfig nalazimo IP adresu Show payloads u MSF komandnoj liniji koja prikazuje listu dostupnih payloada zajedno sa njihovim rejtingom i kratkim opisom. use exploit/multi/http/tomcat_mgr_deploy - aktiviranje aplikacije.

3. **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.

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

SQL injection, CMD izvršavanje, RFI i LFI.