# Part 1: Pentesting

Dear [your name here]

Congratulations on accepting a roll as a web application pentester at Acme Conglomerate Industries!  Many companies pay to have trustworthy employees break into their computers before hackers do. We know you’re one of the best, so we’re happy to have you join the team! Obviously you are excited about starting your Human Resources training.  That 10k page policy isn’t going to read itself!

There has been a change in plans however.

The bad news is that you don’t get to start reading all of those rules till tomorrow.  Sorry about that.  The GOOD news is that the CTO just read an article about a new vulnerability called “Shellshocked.”  We need you to check our network for any servers vulnerable to this “shellshocked” malware!

Your task:

1. Please read up on this vulnerability and determine if we are vulnerable to it.
2. Explain what the problem is
3. Try to determine if we have any servers that are vulnerable to it.
4. Report back to me when you feel you have enough information to determine if we’re vulnerable.

You have permission to scan the network to discover servers & identify if they are vulnerable.

Signed,

Your new boss of pentesting.

# Activity: Determine if your employer has any servers vulnerable to Shellshocked Malware.

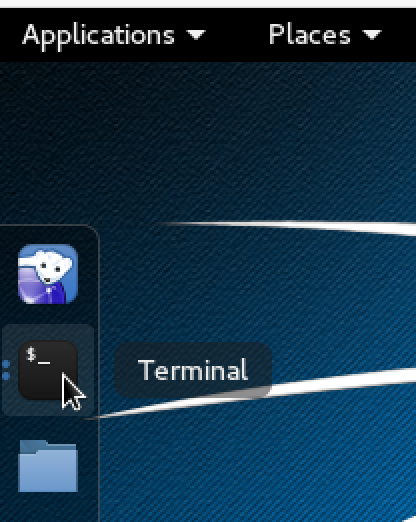
**Step 1: (Optional)** Do a google search for "shellshocked malware."

From Wikipedia:

**Shellshock**, also known as **Bashdoor**, is a family of security bugs in the widely used UNIX BASH shell, the first of which was disclosed on 24 September 2014. Many Internet-facing services, such as some web server deployments, use Bash to process certain requests, allowing an attacker to cause vulnerable versions of Bash to execute arbitrary commands. This can allow an attacker to gain unauthorized access to a computer system

Questions:

* Is Shellshock Malware?
* What is Shellshock?
* What is a shell?
* What is a webserver?
* Why is shellshock bad?
* What does it allow hackers to do?



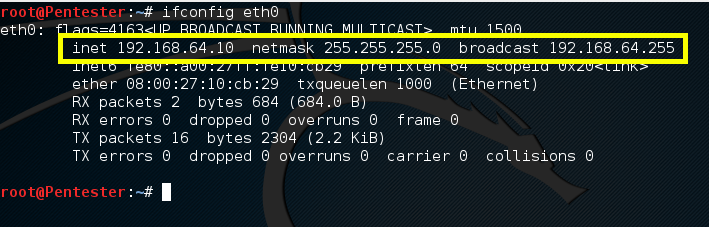
**Step 2a: (Optional)** Scan your network to find all hosts:

First- we need to identify the network we’re going to scan**. We can start this process by identifying our own IP address.**

Open a terminal. You can do this by clicking on the black box in the upper top left hand corner of the pentester VM’s window.

To identify our own IP address, type in the command:

* *ifconfig eth0*



This linux-specific command tells us the ip address of our pentester workstation.

**Every computer on the Internet has an IP address.** Whenever you connect to a web page, you are telling your computer to make a connection to another computer called a web server. Your computer needs to know the address of the destination server in order to make a connection.

It helps to think about mail. How does someone send you a letter? Do they simply write your name on an envelope & drop it off at the post office? Obviously not. They need to write a house number, street name, zip code, city & state. The postal worker then knows how to route the letter as quickly as possible to the receipent.

IP addresses are very similar to postal addresses. They express both the network that a computer is attached to as well as the specific address of the computer. Based on the output of the command above, we can tell that our computer’s IP address is:

192.168.64.10

Alright- we have one address, now we need to figure out the likely other addresses of servers in our network.

With the ifconfic output, we can also see a field called “**netmask**” which has the value 255.255.255.0.

**This tells us that the range of possible computer addresses in our network is 192.168.64.0-255**. A second way of writing this range is 192.168.64.0/24. **We have now identified a network range to scan.**

To scan the network, type the following command:

* *nmap –sn -n 192.168.64.0/24*

Notice that there seems to be a server running on 192.168.64.210.

**Step 2b: (Mandatory):** We found one host that we want to look more closely at 192.168.64.210.

Typing long, complicated commands without making typos is difficult. From here on out, the commands will be automated for you by executing the pentest.sh file.

At the command prompt for the root user at their home directory, type:

*./pentest.sh*

This script takes you through the scanning steps and provides some guidance on what’s happening. Read each section before hitting [Enter]. When you finish running the script, continue on reading the Activity review.

# Activity review:

* What is the “shellshocked” malware?
* Is it malware?
* How does it work?
* What software does it affect?
* How can it be used?
* Did you find servers that were vulnerable?
* What was the IP address of the vulnerable server?
* What URLs on the server were vulnerable to the attack?

Congratulations! You have finished part 1! Good job, Pentester!