

Professional Practices

2021

assignment # 03

# **Ans1:**

**Port Assessment:**

Port assessment is a method of determining which ports on a network are open and could be receiving or sending data. It is also a process for sending packets to specific ports on a host and analyzing responses to identify vulnerabilities. This scanning can’t take place without first identifying a list of active hosts and mapping those hosts to their IP addresses. This activity, called host discovery, starts by doing a network scan. The goal behind port and network scanning is to identify the organization of IP addresses, hosts, and ports to properly determine open or vulnerable server locations and diagnose security levels. Both network and port scanning can reveal the presence of security measures in place such as a firewall between the server and the user’s device. After a thorough network scan is complete and a list of active hosts is compiled, port scanning can take place to identify open ports on a network that may enable unauthorized access.

## Vulnerability Testing

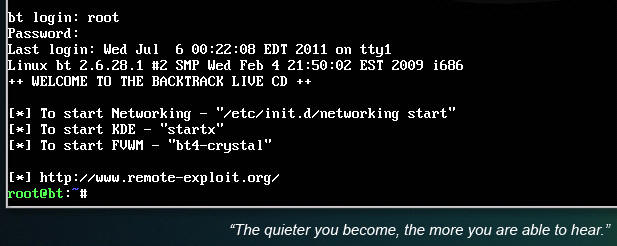
Vulnerability Testing also called Vulnerability Assessment is a process of evaluating security risks in software systems to reduce the probability of threats. The purpose of vulnerability testing is reducing the possibility for intruders/hackers to get unauthorized access of systems. It depends on the mechanism named Vulnerability Assessment and Penetration Testing (VAPT) or VAPT testing. A vulnerability is any mistake or weakness in the system’s security procedures, design, implementation or any internal control that may result in the violation of the system's security policy.

## Example:

**Ans2:**

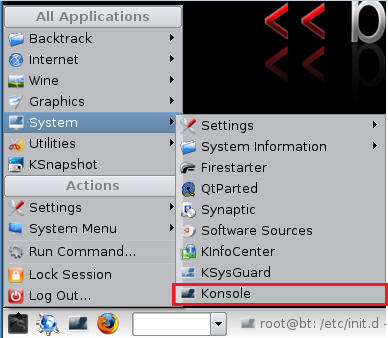
Backtracking is nothing but the modified process of the brute

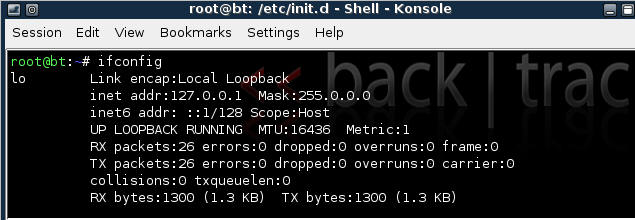
force approach. where the technique systematically searches for a solution to a problem among all available options. It does so by assuming that the solutions are represented by vectors (v., ..., in) of values and by traversing through the domains of the vectors until the solutions is found.

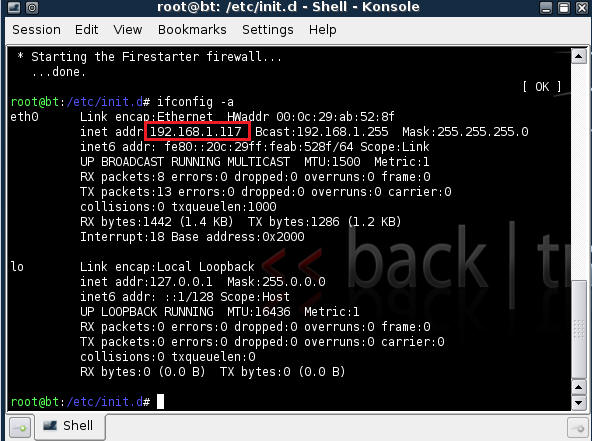
1. Login to your Backtrack01 VM, as username root
   * For those of you that are not a part of my class, the Backtrack01 VM, is BackTrack 4 Linux.
   * 

1. startx
   * Issue the startx command if you are currently are only seeing a console and not a graphical user interface.
   * 

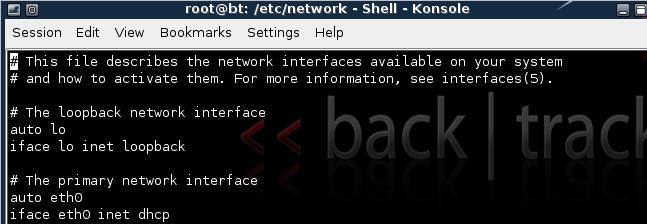
|  |
| --- |
| **2. Confirm Backtrack01 has an IP Address** |

1. Fire up a console or terminal window
   * System --> Konsole
   * 

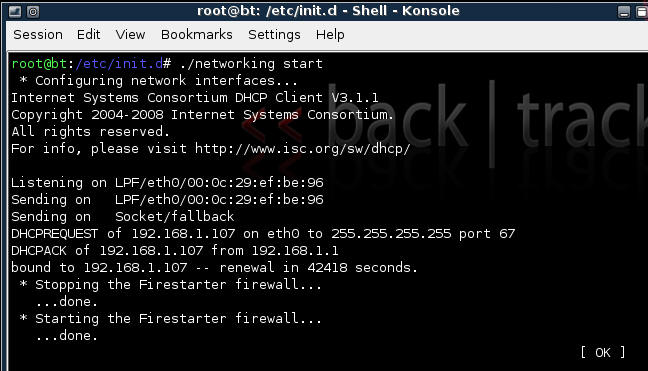
1. ifconfig
   * Example:  No IP Address for eth0
     + If a valid IP address for eth0 is not displayed please move onto step 3.
     + 

* + Example: Valid IP Address for eth0
    - 

1. vi /etc/network/interfaces
   * 

1. Your file should look similar to the below screen shot
   * 

1. cd /etc/init.d/
   * 

1. ./networking start
   * 

1. Confirm you have a valid IP address for eth0
   * In my case, eth0's IP address is 192.168.1.117.
   * 