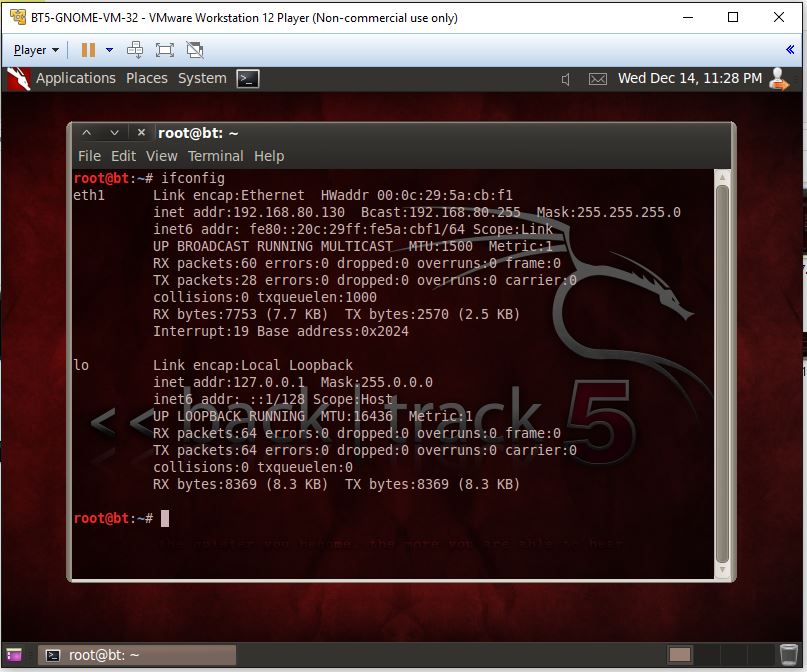
The objective of this example is to demonstrate the steps required for a successful attack against a vulnerable Windows XP SP2 system. It will show: a) how Nessus can be used to discover vulnerabilities in a system, b) how a vulnerability can be exploited using Metasploit, c) the Meterpreter functionality d) a password cracking example, e) the Netcat functionality, f) how an attacker can gain GUI access into a remote system

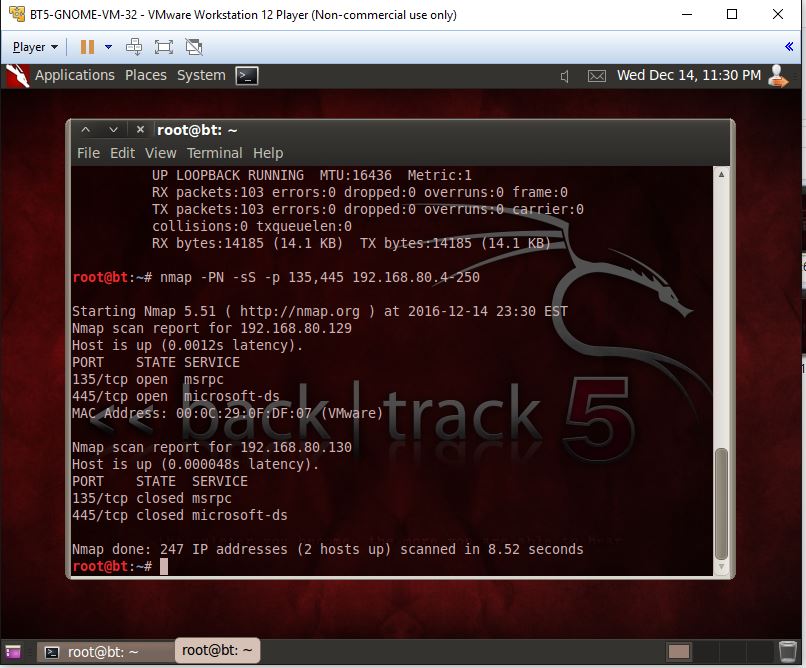
1. Start both **Backtack5 (BT5)** and **Win-XP-SP2** virtual machines. Type their IP addresses. Verify these IP addresses.

We used **ifconfig** to find the ip address of backtrack5. The **IP address** is **192.168.80.130**



Screenshot 1: IP address of Backtrack5 (BT5).

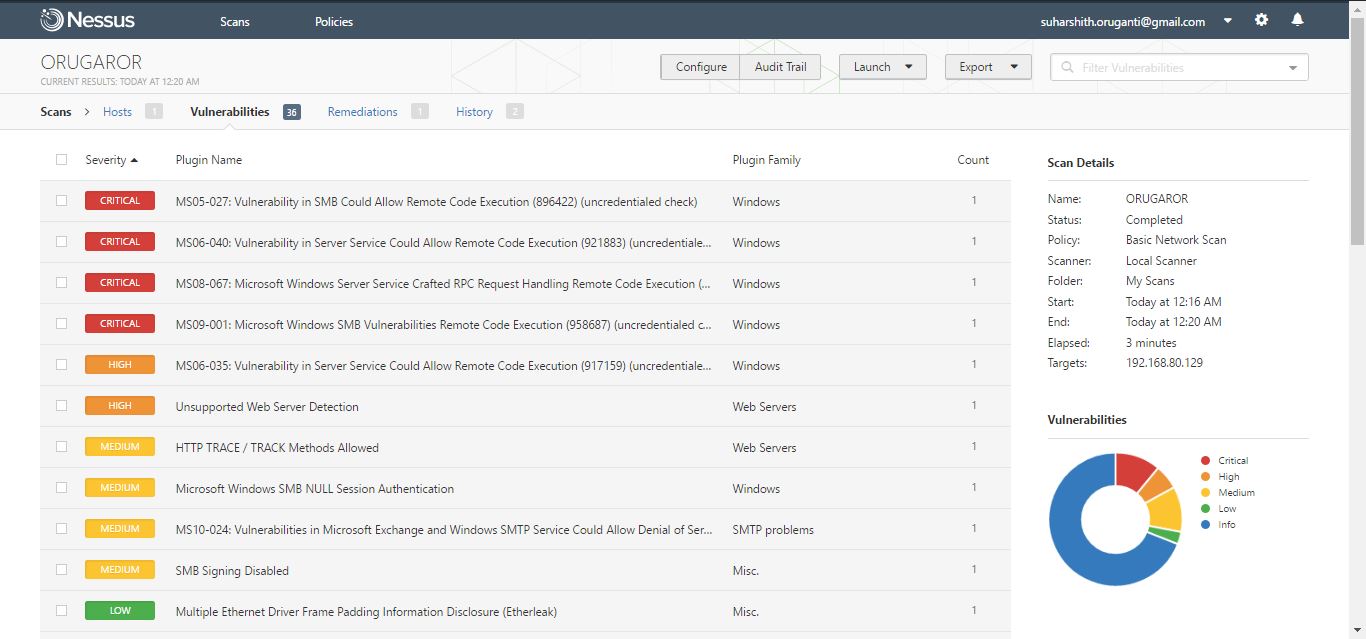
We use nmap command to find the IP address of Win-XP. We give a range of 4-250 to last octet of IP addresses. The result is shown below. Since the **192.168.80.130** is the **IP of Bt5**, then the IP address of Win-XP is **192.168.80.129**



Screenshot 2: IP address of Win-XP-SP2.

1. We used **Nessus** to conduct a **vulnerability analysis** of the **Win-XP-SP2** and **ORUGAROR** both as policy name and as scan name.

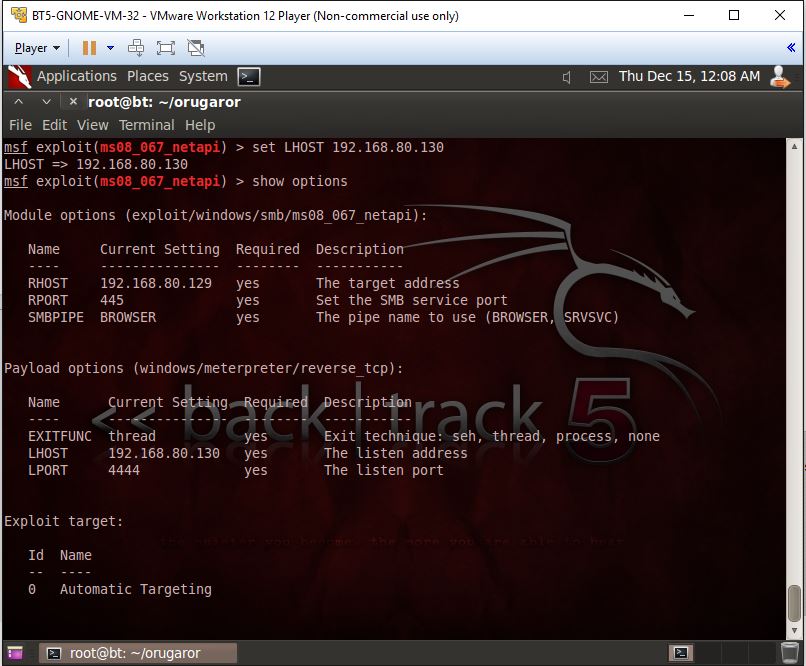
Total 36 Vulnerabilities were found and few of them are as below. The target address is of Windows-XP, **192.168.80.129**



Screenshot 3: Vulnerability analysis of the Win-XP-SP2 using Nessus system.

1. We created a new directory in the root directory of Bt5 with name **orugaror**. Get into this directory and **start msfconsole**. Used the **windows/smb/ms08\_067\_netapi** exploit and **windows/meterpreter/reverse\_tcp** payload to gain access into the Win-XP-SP2 system.

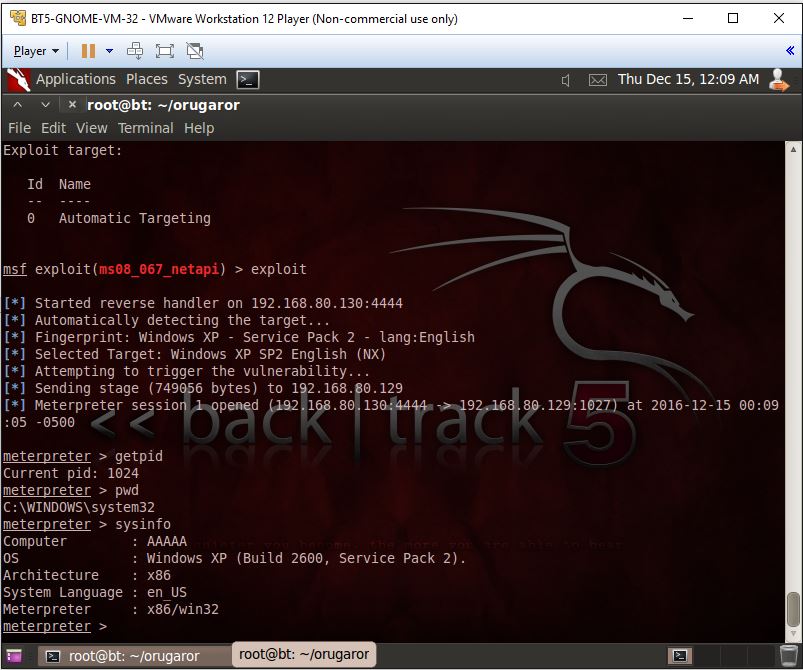
We set **LHOST**, with the **IP address** of bt5 **192.168.80.130** and **show options** command.



Screenshot 4: setting IP address using LHOST and using show options to verify that it has been accepted

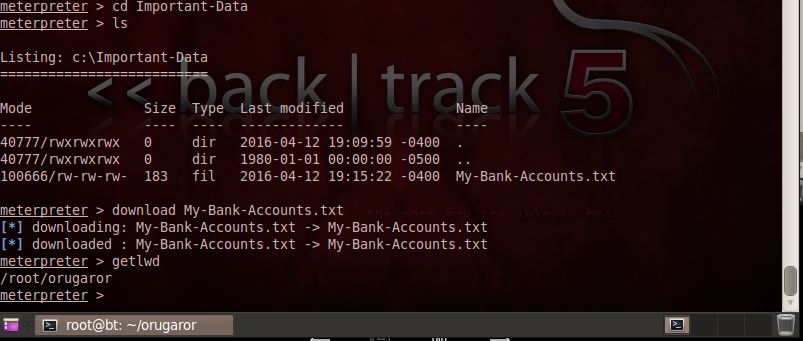
1. We used **exploit** command and it enables us to launch exploit and gain access to Win-XP-SP2. It also shows the exploit was successful and a **meterpreter** **session** was established, then we used **getpid, pwd** and **sysinfo** commands.

The **pid** we got is **1024**.



Screenshot 5: The exploit, getpid, pwd and sysinfo commands.

1. We used the Meterpreter functionality to go to the Important-Data folder of Win-XP-SP2 and download the **My-Bank-Accounts** file to **orugaror** directory of Bt5. We used **cd**, **ls**, **download** and **getlwd** commands and their outputs are shown below.



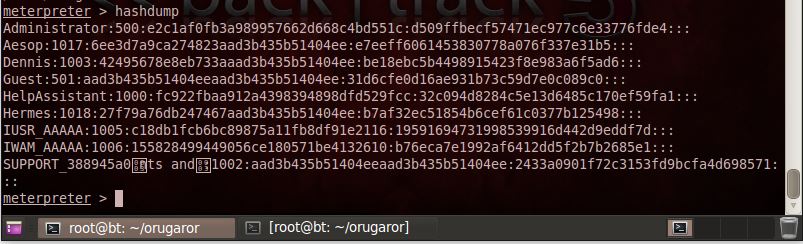
Screenshot 6: Finding and downloading the My-Bank-Accounts.txt file

We used **ls** and **more** commands to view the file which is downloaded.



Screenshot 7: Shows the content of Bank-Accounts.txt file

1. We used **hashdump** to dump the hash values of the Win-XP-SP2 passwords, and then copy them to a file named **Paswd-orugaror** of your Bt5 **orugaror** directory.

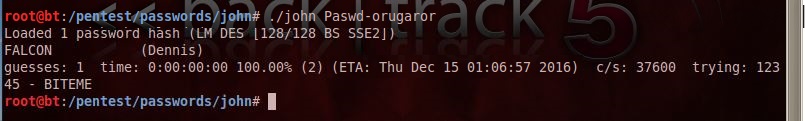


Screenshot 8: Hashdump command and the output.

1. Copy the **Paswd-orugaror** file to John the Ripper directory of Bt5 and use john to crack this file’s passwords; note that in Bt5 **/pentest/passwords/john** is the John the Ripper directory.

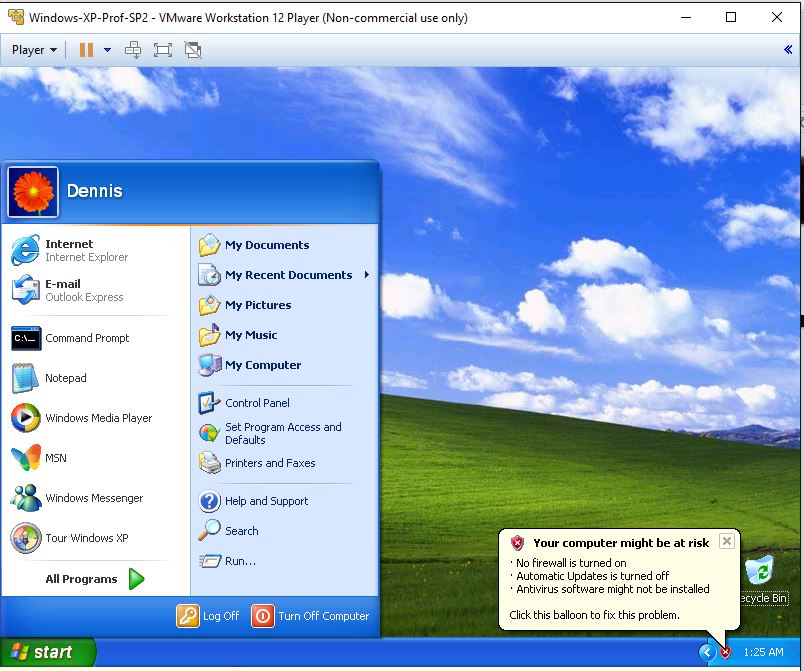


Screenshot 9: Copying Paswd-orugaror file



Screenshot 10: Verifing the Paswd-orugaror file has been transferred to /pentest/passwords/john directory.

1. We used the **Dennis** login name and corresponding cracked password **FALCON** to gain access into Win-XP-SP2



Screenshot 12: Username-Dennis and password-FALCON used to log into the Win XP2 System.