

Windows Assessment Report

CIS 471



Cristian Sierra

00943242

**Overview**

Throughout the quarter we have been working with a Windows 2008 Server to not only learn, but also practice our ethical hacking skills. Some of the tools used to exploit the vulnerabilities found were Kali Linux, Green Bone, Openvas, Metasploit and Armitage. The first step was to upload the 2008 Windows Server to the VMWare Station. The next step was to ping around in Kali Linux to find the target (2008 Windows Server) IP address. Once the targets IP address was found, tools such as Openvas, Green Bone, or Armitage were used to scan for vulnerabilities. Through these tools, some of the vulnerabilities found were MS09-050, FTP, Cracking Passwords, Escalation of Privilege, and Oracle MySQL Security Bypass.

**Vulnerabilities**

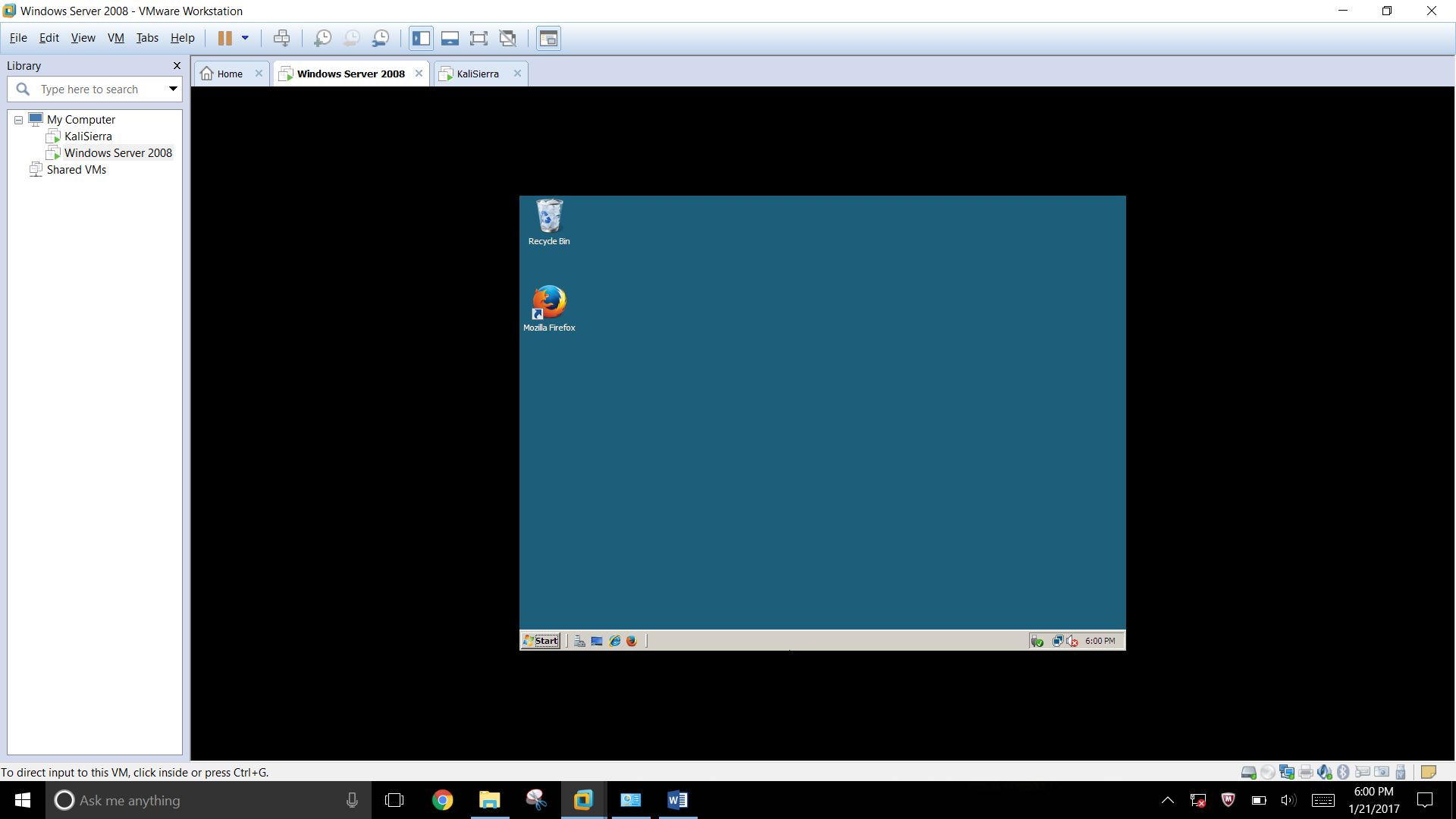
MS09-050:

The third assignment asked to find as many vulnerabilities as possible and to find a way to break into the server. After finding the MS09-050 vulnerability the hacker had the opportunity to reset the Administrator accounts password and login into the server. One way of doing this was to use the terminal on the Linux server and use the “msfconsole” command to prompt metaspolit on the console. The next step was set the RHOST to the targets IP and LHOST to the Linux IP. A shell was then created to penetrate the server and override the Administrator accounts password, which allows the hacker to set a new password.

Solution:

In 2009 Microsoft create an update to fix this problem. The solution would be to check the system for updates to prevent this form happing again.

Proof:



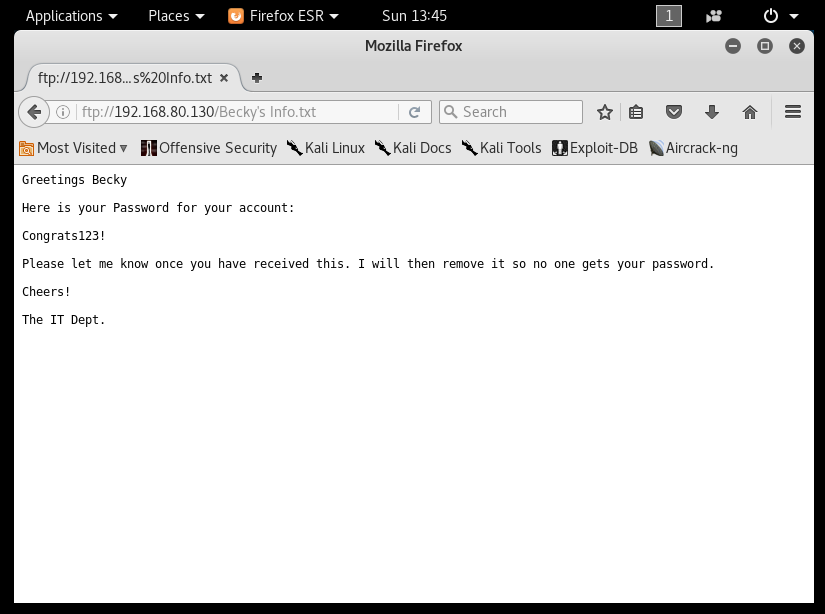
FTP:

For the fourth assignment, a new version of Windows 8 Server was used. This version had fixed the FTP bugs found in the first version that was distributed. Through this, the hacker was able to breaking into Beckys account by an anonymous login through FTP. This was done by opening terminal in Linux and to typing “ftp (target IP address)”. This allowed the hacker to connect to the servers FTP service. The system then asks to input a username and a password, for both fields it did not matter what was typed in. The next step was to open the web browser in Linux and type in the targets IP address. This took the hacker to a webpage where the password for Beckys account was given and allowed the hacker to login into the server once more.

Solution:

A possible solution is to this problem is to turn off anonymous login in the FTP authentication settings.

Proof:



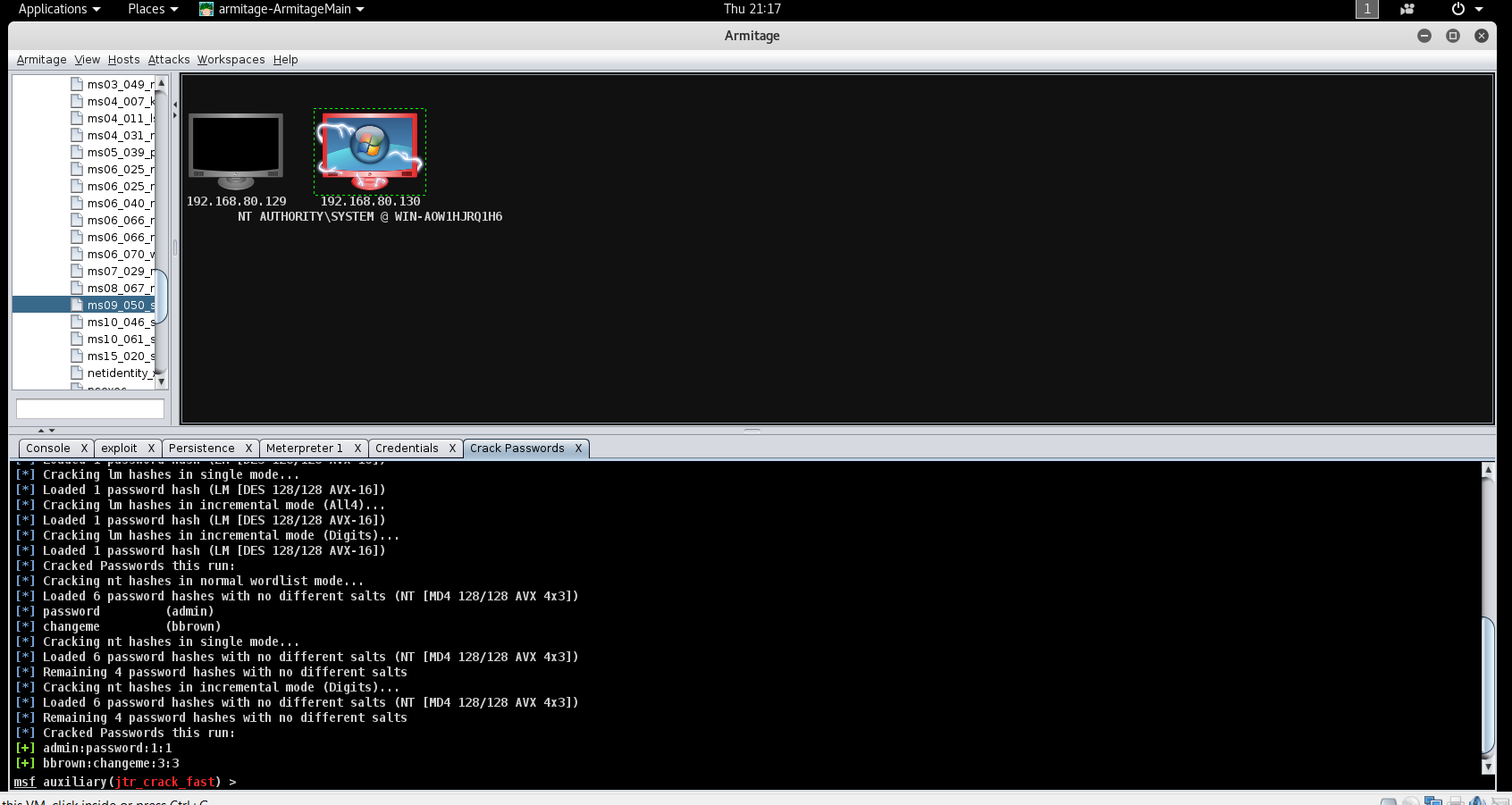
Cracking Passwords:

The first part of the fifth weeks assignment asked to find another way to crack the server and therefor allowed for another way to enter the server. Not only does MS09-050 allow the hacker to rest the Admin account password and allows for privilege escalation, it can also help crack any accounts password. The first step is to crack and dump hashes by using Armitage’s auxiliary script called “jtr\_crack\_fast”. This will give the hacker access to any accounts password that was cracked by Armitage. In this case the BBrowns account was the victim.

Solution:

The solution for this would once again be to check for update to prevent this form happing again.

Proof:



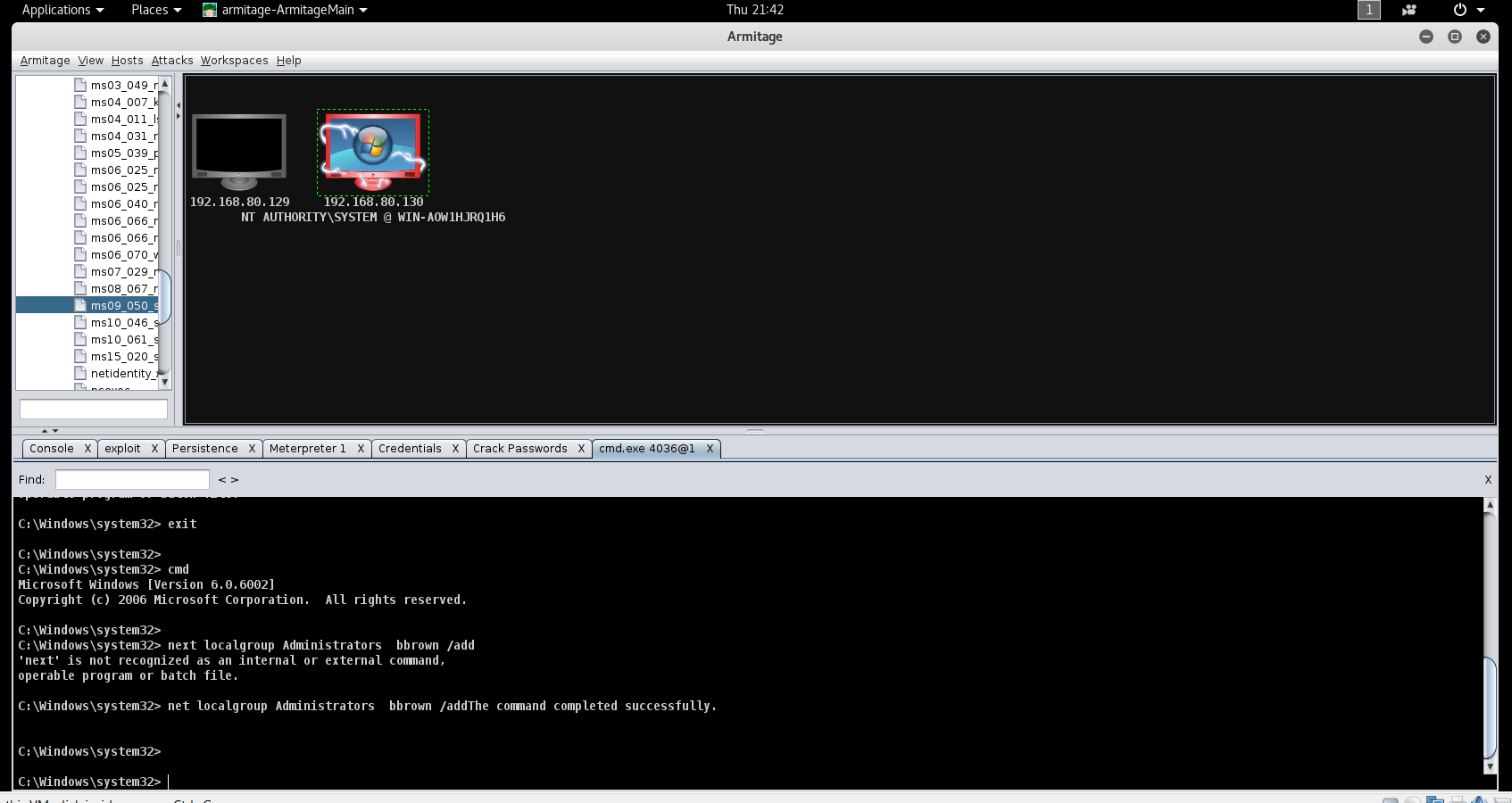
Escalation of Privilege:

The fifth assignment also asked that after breaking into the server once more, to escalate any of the other accounts privileges. Using the MS09-050 vulnerability again, the hacker can login into the target system and grant administrative access to any user. This could be done by first scanning the target vulnerability in Armitage, selecting the MS09-050 vulnerability and then choosing the account to escalate privileges. In this case BBrowns acocunts was the victim. The command that allows this to happen is “next local group Administrator (account that will be escalated)/add”.

Solution:

A simple way of preventing this is to lower the reduce the number of accounts that have administrative access.

Proof:



Oracle MySQL Security Bypass:

When first scanning the system, a large number of vulnerabilities are discovered and are categorized by highest to lowest urgency. The highest one is TCP port 3306, Oracle SQL. This flaw exists because the datadir is writable by the msqld server. This means a user can connect to the MySQL server can create ‘my.cnf’ in the datadir. This impacts the server at the Application Level and is prone to security bypass.

Solution:

Much like MS09-050 all that has to be done is keep the system up to date. Most of the vulnerabilities found on this initial scan can be fixed with keeping the system up to date.