

Linux assessment report

CIS 47



Cristian sierra

009433242

**Overview**

Throughout the second half of the quarter, we had to work with a Metasploitable 2 Server to keep building upon our ethical hacking skills. Some of the tools used to exploit the vulnerabilities found were Kali Linux, Green Bone, Openvas, Armitage and Hydra-gtk. The first step was to upload the a Metasploitable 2 Server to the VMWare Station. The next step was to ping around in Kali Linux to find the targets (Metasploitable 2 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 vsftpd\_234\_backdoor, unreal\_ircd\_3281\_backdoor, vulnerable web services,

**Vulnerabilities**

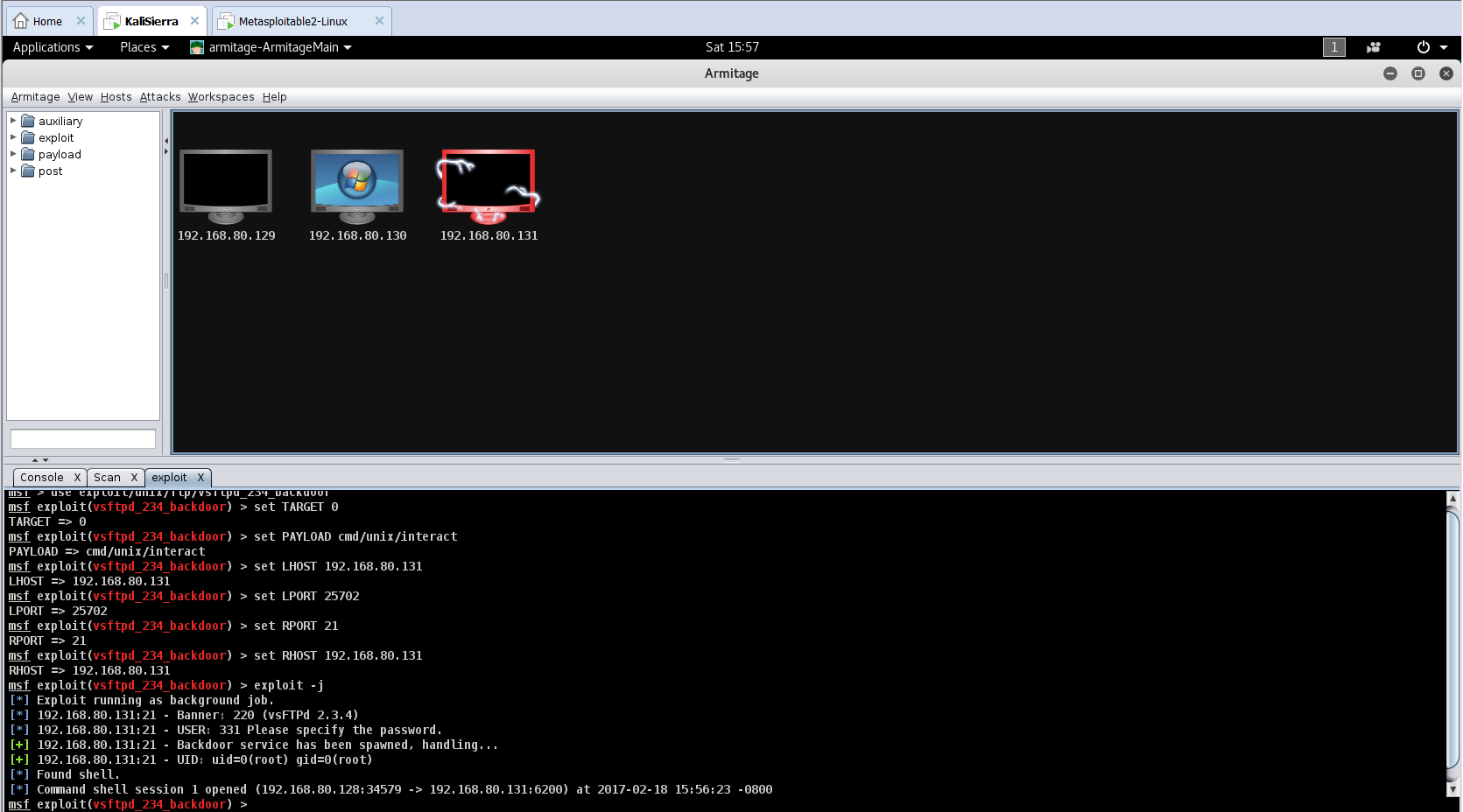
*vsftpd\_234\_backdoor – Port 21*

On the second assignment where we had to use Metasplotiable 2, we had to find and execute any vulnerability to grant the hacker backdoor access. vsftpd stands for Very Secure FTP Daemon and it is found in FTP servers for Unix-like systems. vsftpd\_234\_backdoor exploits a malicious backdoor that was added to the VSFTPD download archive when it was first created. Attackers can exploit this issue to execute arbitrary commands in the context of the application. If the attack is successful, it will compromise the affected application. This was found in Armitage by first scanning the targets computer for attacks and then selecting the vsftpd\_234\_backdoor option under the ftp tab.

Solutions:

In July of 2011 this backdoor was removed. The solution for this problem would be to check the system for updates to prevent this from happening again.

Proof:



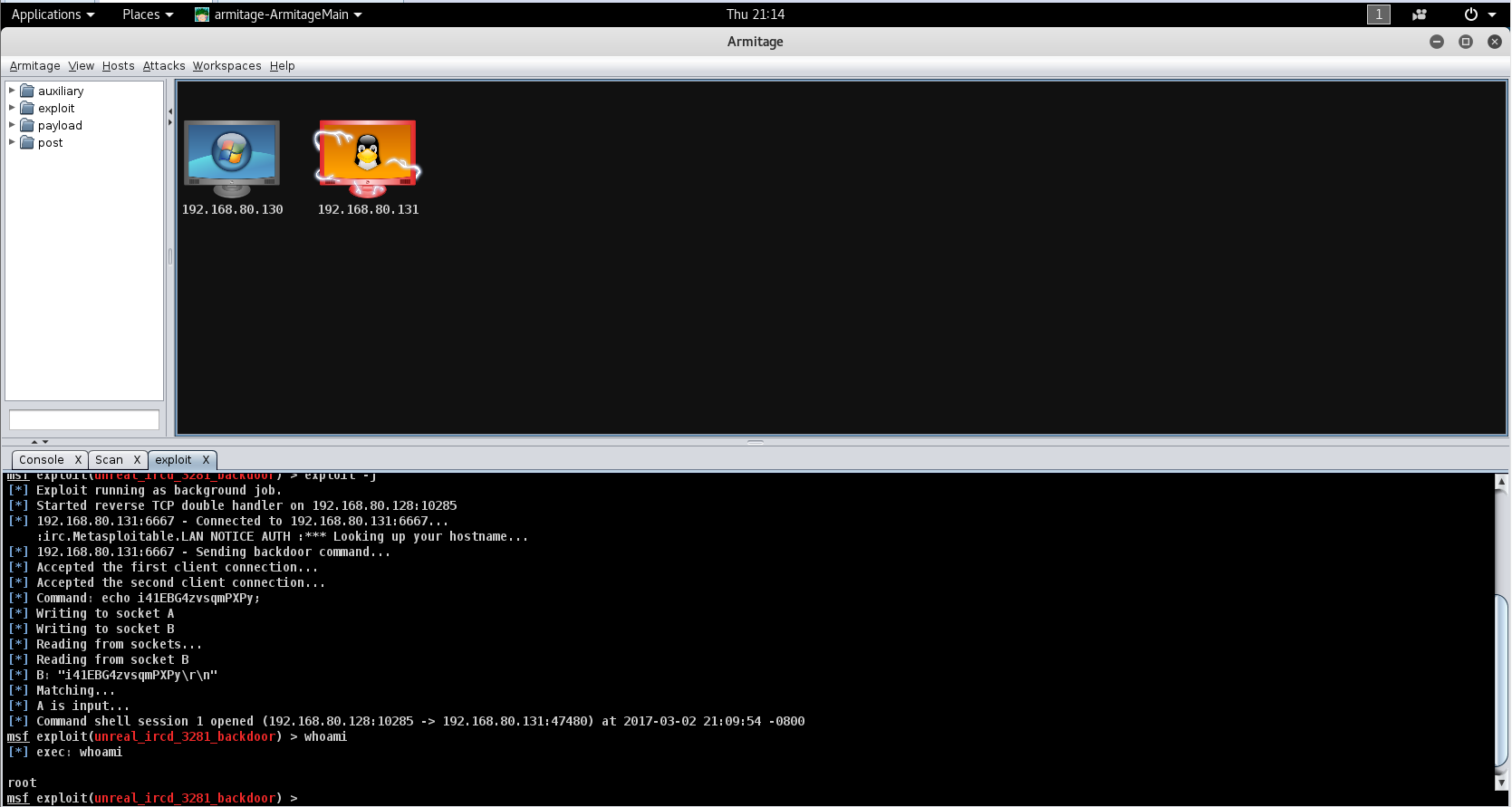
*unreal\_ircd\_3281\_backdoor*

UnrealIRCd is an open source IRC daemon that is available for Unix-like operating systems and Windows. Since the beginning of development on UnrealIRCd, many new features have been added and modified, including advanced security features and bug fixes, and it has become a popular server. If the hacker successfully exploits this vulnerability, the hacker will have full access to the server. This was found in Armitage in the attacks tab under the irc option.

Solution:

The solution for this problem, once again, would be to check the system for updates to prevent this from happening again.

Proof:



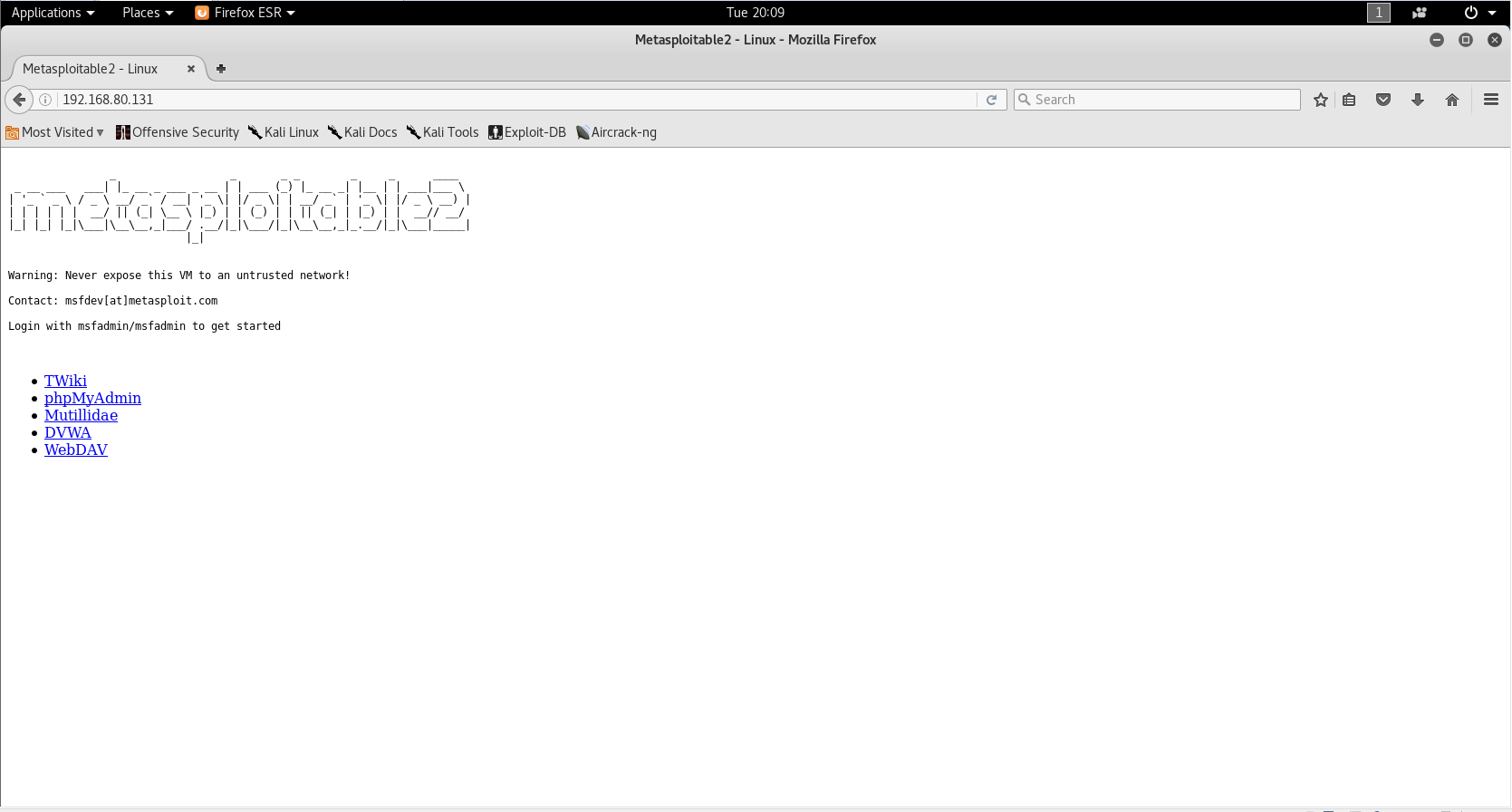
*Vulnerable Web Service*

Metasplotiable 2 Server has a purposely vulnerable web application that is pre-installed. This web server starts automatically when Metasplotiable 2 Server is booted. To access this particular web application, the hacker has to open up a web browser in Kali Linux and then type in the targets IP Address. If the attack is successful the hacker will have access to servers username and password and other important information. This could let attackers steal cookie-based authentication credentials or compromise affected application.

Solution:

There is an upgrade through VendorFix that will remove this vulnerability. The solution for this problem would be to check the system for updates to prevent this from happening again.

Proof:

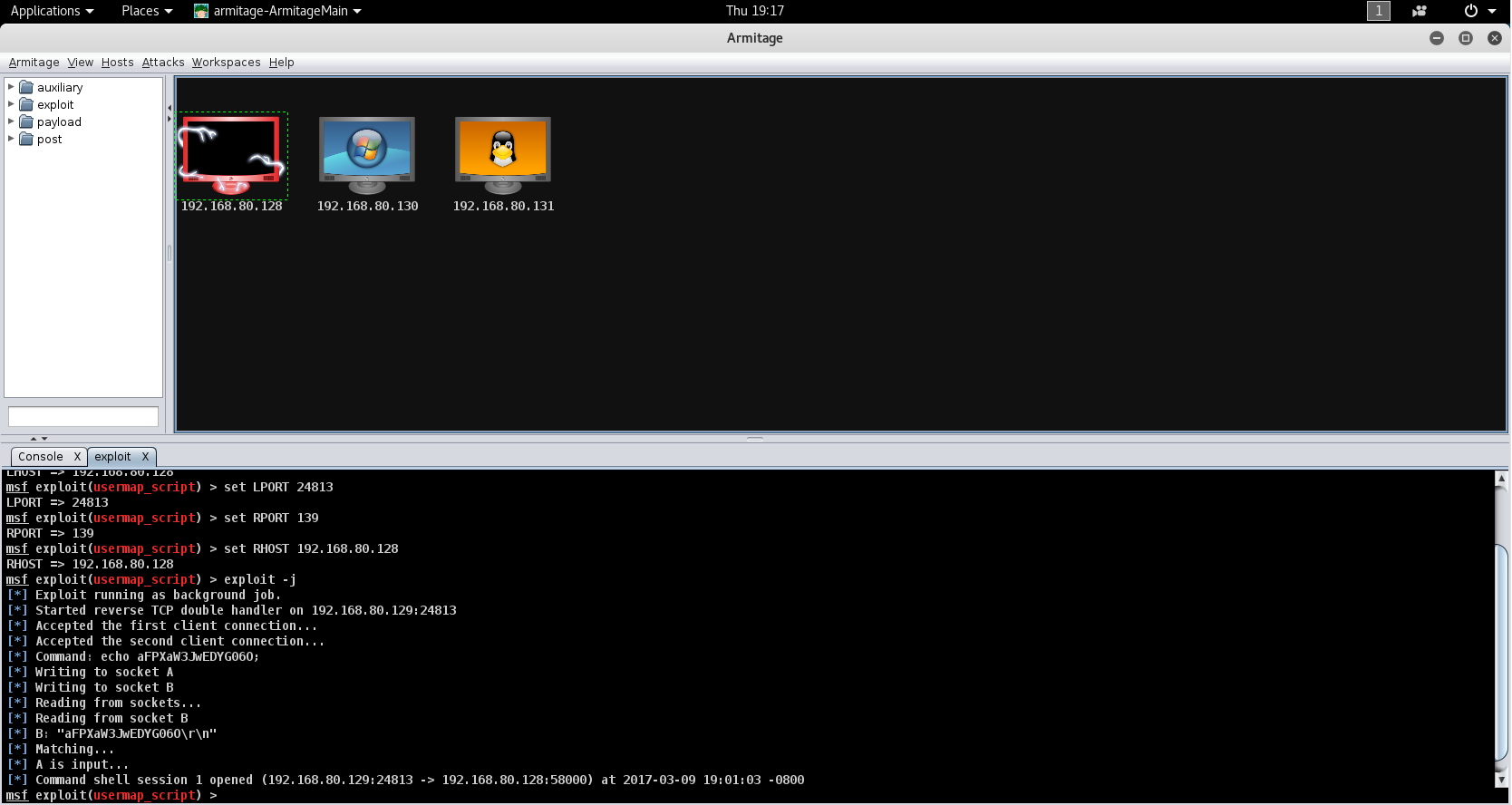


*Samba usermap\_script*

This exploits a command executing a vulnerability in Samba using the non-default “username map script” configuration option. By using a specific username containing a shell meta characters, attackers can execute this arbitrary command. Since no authentication is needed to exploit this vulnerability, this option is used to map usernames prior to authentication.

Solution:

Once again to update the system using VendorFix.



*NVT: Java RMI Server Insecure Default Configuration Remote Code Execution*

This vulnerability attacks Java products that implement the RMI Server that contains a vulnerability that could allow an unauthenticated, remote attacker to execute arbitrary code on a targeted system with elevated privileges. The vulnerability exists because of an incorrect default configuration of the Remote Method Invocation (RMI) Server in the affected software.

Solution:

The solution is to work around by disabling class-loading.