VAPT Test Report

**Name : Karthik Narayanan A**

**Email :** [**karthiknarayanan.cse2021@citchennai.net**](mailto:karthiknarayanan.cse2021@citchennai.net)

**Regno : 210421104074**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | 1. Initializing the academy VMmachine1.1 Turning on network device ens33 on academy machine **Problem Explanation:** By default the ens network service on the acdemy machine will be in the state down. So our academy machines Ip address will be disabled  **Problem Fix:** This problem can be fixed by properly configuring the network interfaces file that is found in our Debian machine.  **Steps to fix the problem:** This problem can be fixed by making some changes in the interfaces file which can be found in the directory ‘ /etc/network’. 1.2 Configuring the interfaces file We can use nano to edit the interfaces file. Initially the interfaces file will look like this    Then we need to change all the network interfaces in the mentioned file to ens 33 network.  After changing them our interfaces file should look like this    After changing when we check the ip address using the following command  └─$ ip address  Now the ip address for our academy machine will be displayed and It will be whthin the same subnet of our windows machine.    **1.3 Installing Splunk Universal Forwarder :**  After creating a network connection to our Academy machine we need to set it to bridge network to enable ssh access to other devices.  Now we need to install Splunk Universal Forwarder on our academy machine si that we can send logs to our splunk cloud device.  For that we need to install splunk universal forwarder for our linux machine by copying the command line which will be given on the downloading page.  └─$ wget -O splunkforwarder<version name> “splunk\_forwarder\_url”    After the .deb file for the splunkforwarder has been installed we need to depackage the splunk universal forwarder deb file. The command used to dpkg the file are  dpkg -i <directory\_of\_splunkforwarder.deb\_file>  now to can see that our splunk forwarder has been automatically initialized in the ‘/opt’ directory.    Now we have to change the ownership of splunkforwarder to the user splunkfwd by using the chown command  chown -R splunkfwd:splunkfwd /opt/splunkforwarder  **1.4 Configuring Splunk cloud** :  Now after the splunk forwarder has been installed we need the import the cloud crendentials package for our splunk cloud credentials package to our academy machine to connect splunk forwarder to our splunk cloud.  After downloading the splunk cloud credentials which will be of the name splukclouduf.spl we need to import the file to our academy machine.  This can be done by using the scp command which can be used to transfer files from one network to other network. The command line for scp is given as  scp filename hostname@host\_ip\_addres:/<directory\_in\_host\_machine>  After entering the password of our academy machine we can see that the file has been successfully transferred.  Now we have to add a forward server for our universal forwarder and configure its port number which can be done with the command after navigating to the bin directory in the splunk forwarder. By default the forwarding server will be 9997.  ./splunk add forward-server <user\_name>:<forwarding\_port\_number>  After we have set up our forwarding server we have to deploy our receiving port.By default the receiving port will be 8089.  ./splunk set deploy-poll <user\_name>:<receiveing\_port\_number>  Now we have to send the log files which is found in our /var/log directory which we have to monitor to our cloud which can be done by using the command  ./splunk add monitor /var/log  The commands for all the splunk is given in the below image    Now we can see our academy machine instance added to our splunk cloud.      This is the event log of the academy machine which can be found in the splunk cloud after enabling the forwarder service.  **2.Attacking phase :**  After we have set up our cloud now we have to start the apache2 server on the academy machine so that we can access the web page which is found in the academy machine. The command for starting the apache2 server is  systemctl start apache2  Now having the webserver running we can access the webpage which can be accessed by entering the academy ip on the webpage of the given browser(firefox).  Now we need to find all the directories that are available within the server using the wfuzz.    Now we have found the academy directory that is available in the apache webserver.  After giving the directory /academy we can find the student registration page in which we need to enter the login credentials.    **2.1. Finding Open Ports and Sevices :**  Now we need to find the open ports and services which are in the webserver. To do this we can use the network mapping command in the linux.  The command to find the open ports is  nmap <ip> -p- -v    Now we can see that ports 21,22,80 are open on the web server.  We can see that the service opened on the port 21 is ftp , in port 21 is ssh and port 80 is http.  **2.2 FTP Accessing**  Which means we can have ftp access to our academy ip. We can access the using the ftp along with the academy ip  ftp><academy\_ip>    Since our academy is an anonymous port we can access it through by using the username anonymous and password as [anonymous@gmail.com](mailto:anonymous@gmail.com)    We can find that the note.txt is found in the ftp. We need to transfer this note.txt to our kali machine which can be done by using get command  get note.txt  After getting the note.txt on our kali machine on the we can find the student name and password in the given query which can be found on the file.    Now we need to crack the hash to find the password of the student credential as we already have the student regno (‘10201321’) to login.  We can use john the ripper to crack the password of the hash. The john command for cracking the hash is  john –word-list=<wordlist\_directory> --format==raw-md5 <hashfile>  Where the word list is the default rockyou.txt which can be found in kali and the hashfile should contain the hash of the password. After running it we can find that the password is student.    **Accessing the web-server as a user :**  Now we have to access the web page using the credentials we have have found. After logging into the webpage we can see that in My Profile page in the academy directory has a page in which we can upload our file into it.  After that we find that the any file can be uploaded into the photo upload input field.  **2.3 Reverse Shell:**  Now we can use this vulnerability to upload a reverse shell script which can give access to the academy machine. The reverse shell script can be found in the kali by default. Where we have to configure the ip our Kali machine so that we will get access to the shell of the webserver after the webserver executes the given file.  The directory for finding the reverse webshell script can be found in usr/share/webshell/php..    This is the reverse-shell php script which we are going to upload and the listening port number is 1234.  The listening can be done with the following command  nc -lvnp 1234  After uploading we can see that our kali has got the access to the academy ip and our shell is currently displaying the academy shell.  **2.4 Horizontal Privilege access:**  Now we can find the users which can be found in the academy machine.By checking the etc/passwd file.    We can find that the academy machine has the user grimmie , splunkfwd which is for splunk forwarder.  Now we need to find the grimmie’s password so we can switch to grimmie user.  After the digging through the file we can find a very suspicious file which contains his mysql username and a password. The folder which contains the file is ‘/var/www/html/academy/includes’ in that the config.php has all these information.    Since it the user name is given as grimmie we can check and see whether the username grimmie has the same password as that of the sql password.  Now we can try to ssh to grimmie user using the grimmie’s password by giving the following command  ssh grimmie@<academy\_ip>  Where my academy ip is 192.168.1.39 and when it asks for the password we can give the password as My\_V3ryS3cur3\_P4ss.  You can see that our shell will be with the username grimmie.  **2.5 Vertical Privilege Escalation:**  Now by using grimmie we need to find any vulnerable files which can be used to gain the root access to our machine. To do this we can use the linPeas to get the folder which are vulnerable and not properly given permission management.  The linPeas can be found in the github. We can download the linPeas.sh file from the github and use the command to execute linPeas file.  After the execution of linPeas we can find that the academy machine has a file called backup.sh which can be found in the directory /home/grimme and the backup.sh file is cronjob file which means that the backup file will be executed automatically during regular intervals of time.    From the above image we can see that backup.sh is administered by the root process.  Now we can write a reverse shell script in this backup.sh file so that we will be able to get access to the root privilege of the academy machine.  By using the reverseshell generator website we can create a script and edit the script into backup.sh file. After introducing the revershell script our backup.sh file would look like this    Where the ip is the ip address of our kali ip and I configured the listening port as 9001.  Now we need to make our backup.sh as an executable file so that it will be executed by the root machine and we can get an access to the root administrator.  To do this we can use the chmod command in linux  chmod +x backup.sh  Now the details for our backup.sh file should look something like this    After saving the file we need to enable the listener in our kali machine.    After some time we can see that our kali machine has been configured to the root user of the academy machine.  **2.6 Accessing Files in Academy Machine :**  Since we are logged in as a root in the academy machine we will have privileges to access any file in the machine.  After listing the files in the / folder of the we can find the flag.txt file.  After that we can read the flag file to read the hidden message.    Now we have finally accessed the flag.txt file in the academy machine.    ------------------------------------------------------------------------- |  | |  | | |  |