Lab Report 6

1. Assessment Sheet
2. **What is the purpose of the business impact analysis (BIA)?**

The purpose of the BIA document is to determine the impact to an organization in the event that key processes and technology are not available.

1. **What is the difference between a disaster recovery plan (DRP) and a business continuity plan?**

In the BIA, the BCP is a prior step of DRP. BCP gives a plan on how to continue business after the event and it specifies responsibility and supporting structures. DRP gives the specific procedures that how we can get system back to normal especially when bad things happen.

1. **What are the commands used in Windows 2012 to mount the NFS share on the Linux server.**

mount -o mtype=hard 172.30.0.200:/var/www \*

1. **Is creating redundancy for systems such as Active Directory or Web servers a part of the DRP or the BCP?**

Yes, it’s part of BCP. DRP is focusing on the recovery process.

1. **Why use the mklink command?**

The mklink command will create a symbolic link and through this link we can access remote drive as local folder. Furthermore, this kind of link can enable tools like xcopy to work on remote drives by making them visible to the local OS.

1. **What role/service is Windows 2012 Server Backup part of?**
2. **Windows Group Policy**
3. **Windows Collaboration Server**
4. **Windows Server Essentials Experience**

**Answer:** C

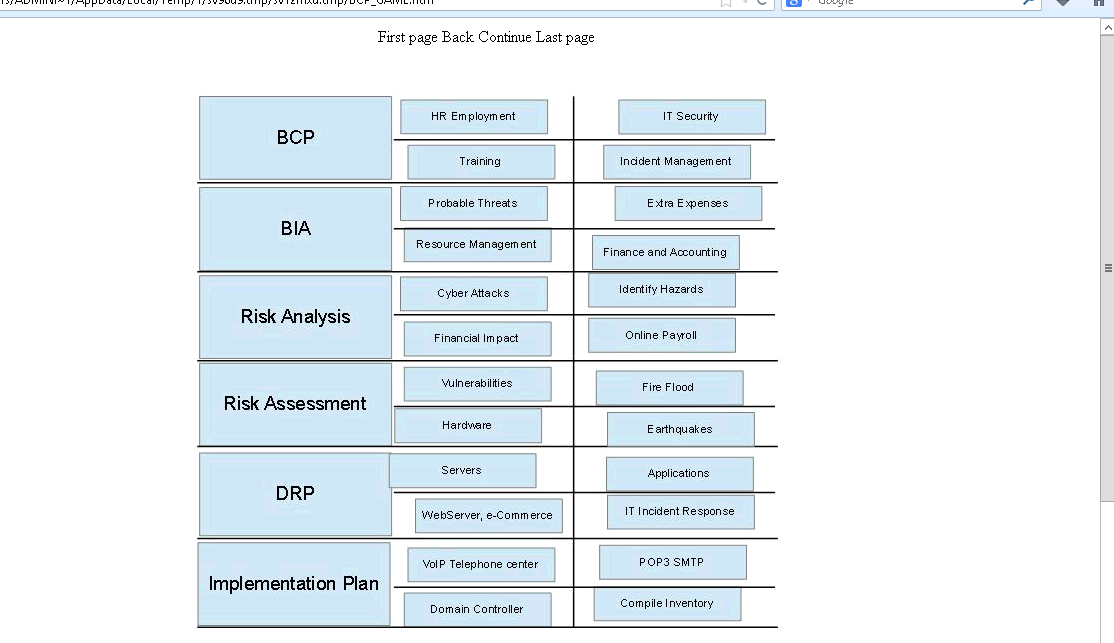
1. **Which Linux file makes a local share available to NFS client?**
2. **transports**
3. **imports**
4. **fstab**
5. **exports**

**Answer:** D

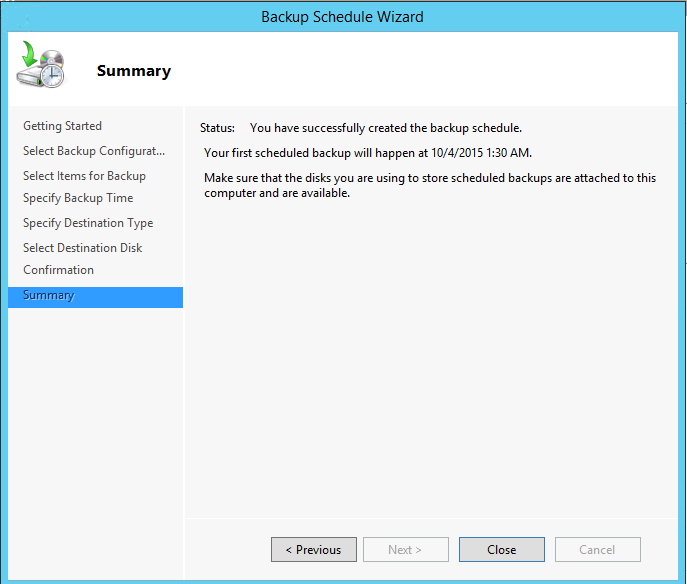
1. Challenge Questions

**Description: Finish the game board and provide screenshot, prioritize the activities listed for SweetThings.**

1. Game Board



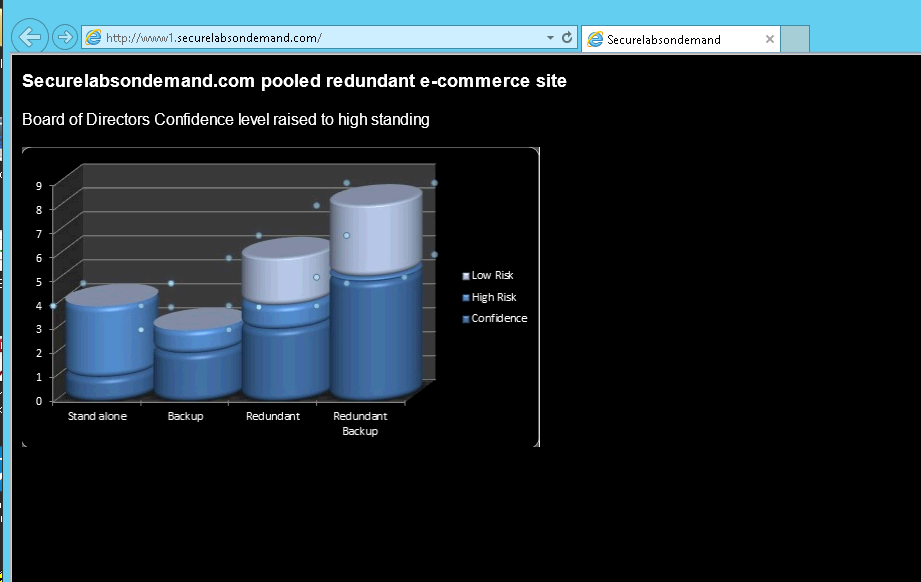
1. Sweet Things priority
2. Report Screenshot
3. Webadmin GUI scheduled backup summary page



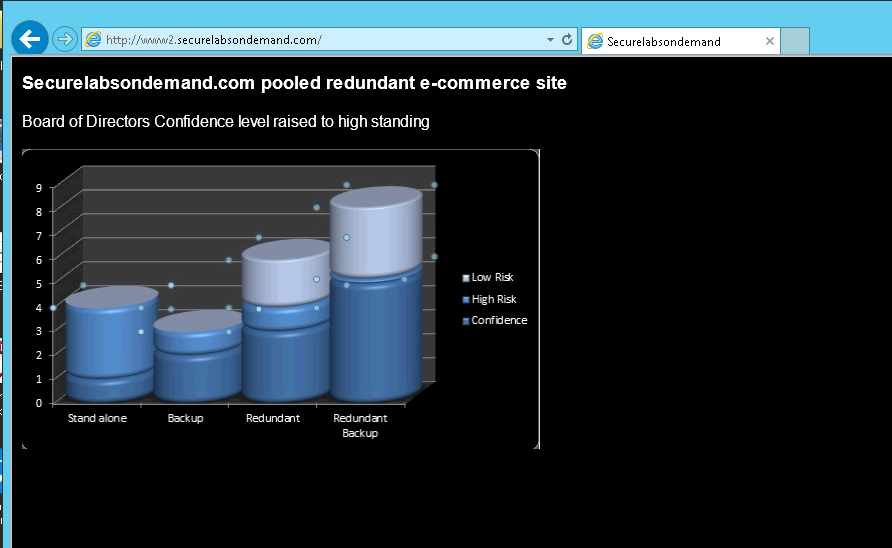
Explanation:

This figure shows that we have already successfully set up the backup schedule by using webadmin GUI tools that are provided by Windows Server.

1. NTF Share – Updated Web content
2. www1 content change



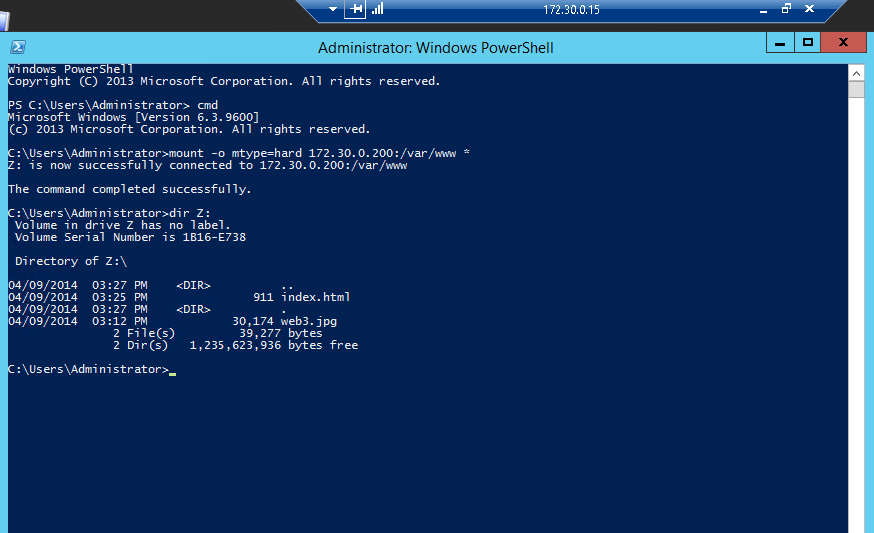
1. www2 content change



Explanation:

In this step, we changed the mount options in the configuration file fstab under /etc folder. And, the content of the web site is changed because different background files are applied to it because the files’ path has been changed.

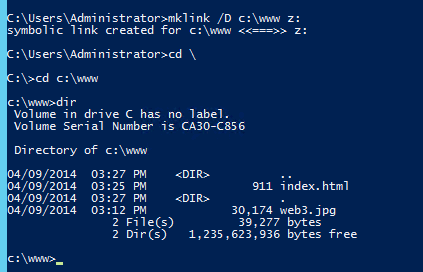
1. Contents of Z: directory



Explanation:

From this figure, we can see some files and directories which are used to store the web application for two sites – www1.securelabsondemand.com and www2.securelabsondemand.com.

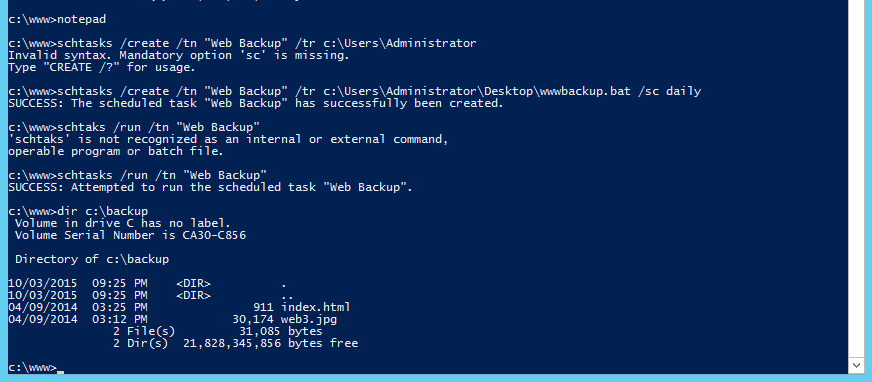
1. Contents of c:\www directory



Explanation:

In this step, we linked the remote server’s folder to our local folder. So, we can access the remote folder as the same way of accessing our local folder.

1. Contents of the c:\backup directory



Explanation:

In this step we create a schedule task which is used to perform a backup activity. The backup commands are written in wwwbakup.bat batch file. And then we manually execute the scheduled task and after the task successfully is executed, we can see all the files on the server that are need to be backup now are copied to our local computer’s backup folder.

1. Other additional supporting text/image content

Lab Report 14

1. Assessment Sheet
2. **What are the five steps of ethical hacking**

The five steps are reconnaissance, scan target, vulnerability analysis, exploitation and post-attack activities.

1. **During the reconnaissance step of the attack, what open ports were discovered by Zenmap? What Services were running on those ports?**

During the reconnaissance step, from the result of Zenmap, we found total 23 open ports and each port provides a specific services. These open ports and services are list below

|  |  |  |  |
| --- | --- | --- | --- |
| Port | Protocol | State | Services |
| 21 | Tcp | open | ftp |
| 22 | Tcp | Open | ssh |
| 23 | Tcp | Open | telnet |
| 25 | Tcp | Open | smtp |
| 53 | Tcp | Open | domain |
| 80 | Tcp | Open | http |
| 111 | Tcp | Open | rpcbind |
| 139 | Tcp | Open | netbios-ssn |
| 445 | Tcp | Open | netbios-ssn |
| 512 | Tcp | Open | exec |
| 513 | Tcp | Open | login |
| 514 | Tcp | Open | shell |
| 1099 | Tcp | Open | java-rmi |
| 1524 | Tcp | Open | shell |
| 2049 | Tcp | Open | nfs |
| 2121 | Tcp | Open | ftp |
| 3306 | Tcp | Open | mysql |
| 5432 | Tcp | Open | postgresql |
| 5900 | Tcp | Open | vnc |
| 6000 | Tcp | Open | X11 |
| 6667 | Tcp | Open | irc |
| 8009 | Tcp | Open | ajp13 |
| 8180 | Tcp | Open | http |

1. **What step in the hacking attack process uses Zenmap?**

We use Zenmap in the reconnaissance stage of hacking attack process because it returns the information about possible OS of target, the currently running services and open ports. Based on this information, we can do next step to further explore the potential weakness of our system.

1. **What step in the hacking attack process identifies known vulnerabilities?**

Basically, we identify the vulnerabilities in the step of scan target and after finishing the scanning, we will do analysis of these vulnerabilities, which represents that we are in vulnerability analysis step.

1. **During the vulnerability scan, you identified a vulnerable service in the Linux victim system. What was the name of the vulnerable service?**

The name of the vulnerable service is called vsftpd. The full name of this vulnerability is NVT: vsftpd Compromised Source Packages Backdoor Vulnerability.

1. **If you are a member of a security penetration testing team, and you identify vulnerabilities and exploits, should you obtain written permission from the owners prior to compromising and exploiting the known vulnerability?**

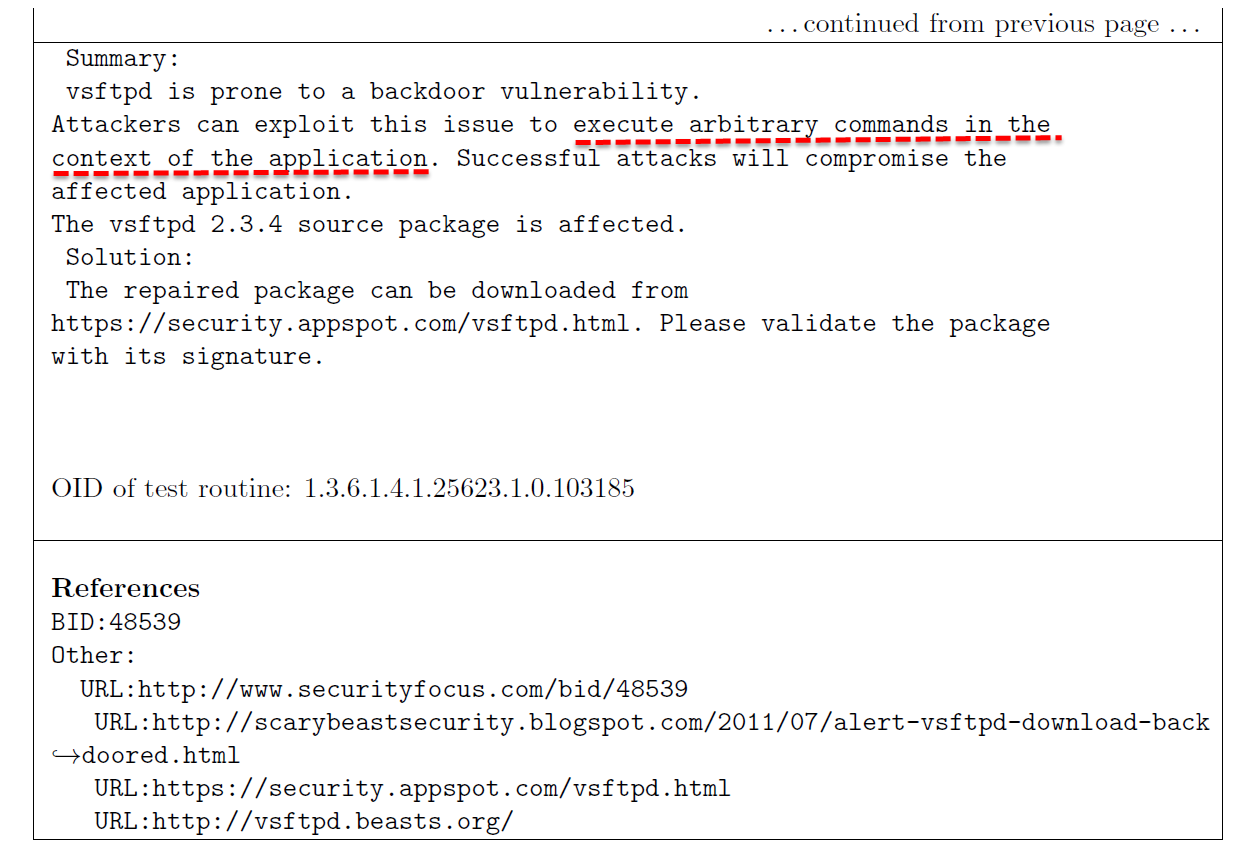
Of course as an ethical hacker, before we do anything to our client, we should ask written permission first. Without this permission ethical hacker becomes an attacker which might be arrested by government agency because the unauthorized hacking is illegal.

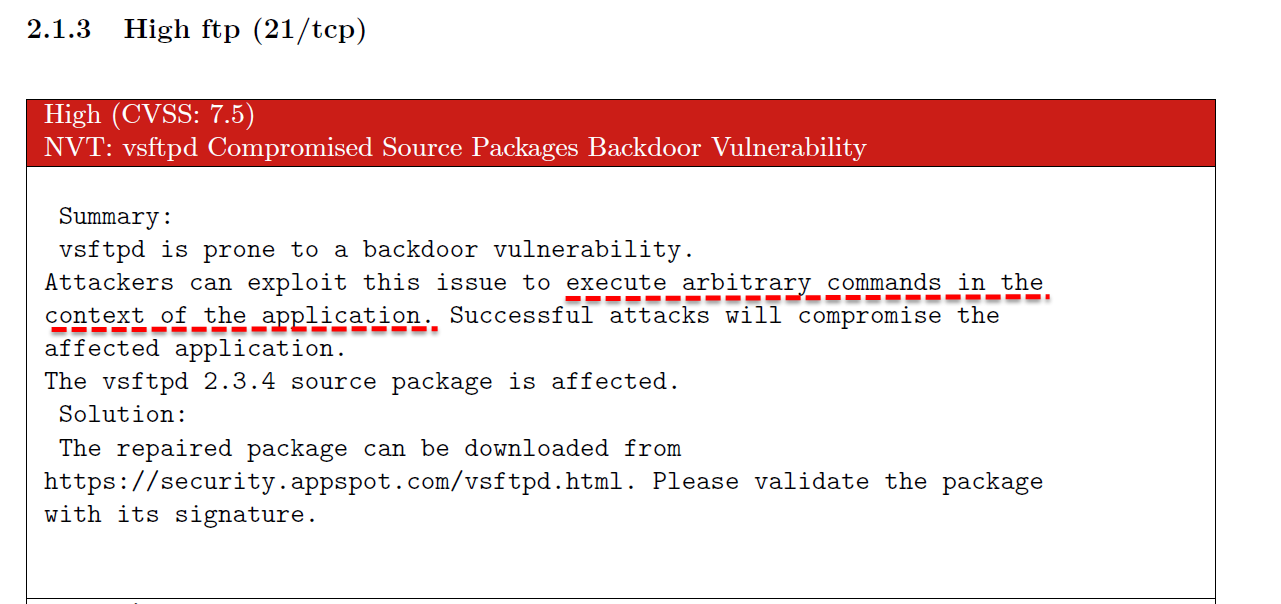
1. Challenge Questions

**Description: Find the vulnerability in the normal lib exercise which allows attacker to remotely execute shell. Use Metasploit to exploit the vulnerability and document the successful exploitation. Research the vendor of the software that the software needs to be patched and include the download URL for the patch.**

1. Identify the vulnerability

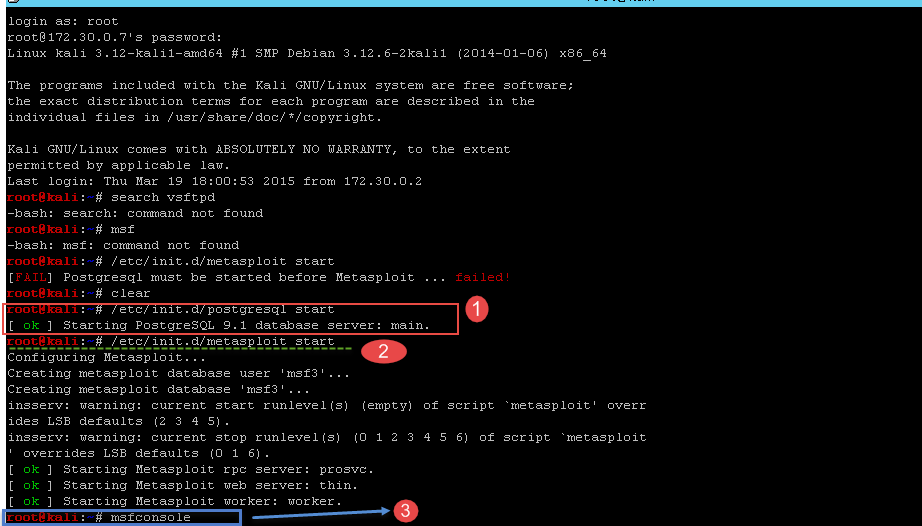
Within the OpenVAS report that we downloaded for IP address 172.30.0.30, we could found many vulnerabilities and some of them are marked as high risk. In these high risk vulnerabilities, we could found that there is a vulnerability related to vsfpd production and it appears in two kinds of services – clm\_pts (port 6200/TCP) and ftp (port 21/ tcp). The negative impact of this vulnerability is that it allows the attackers to remotely execute commands under the context of vsfpd software. The two services impacted are showed as following two pictures.



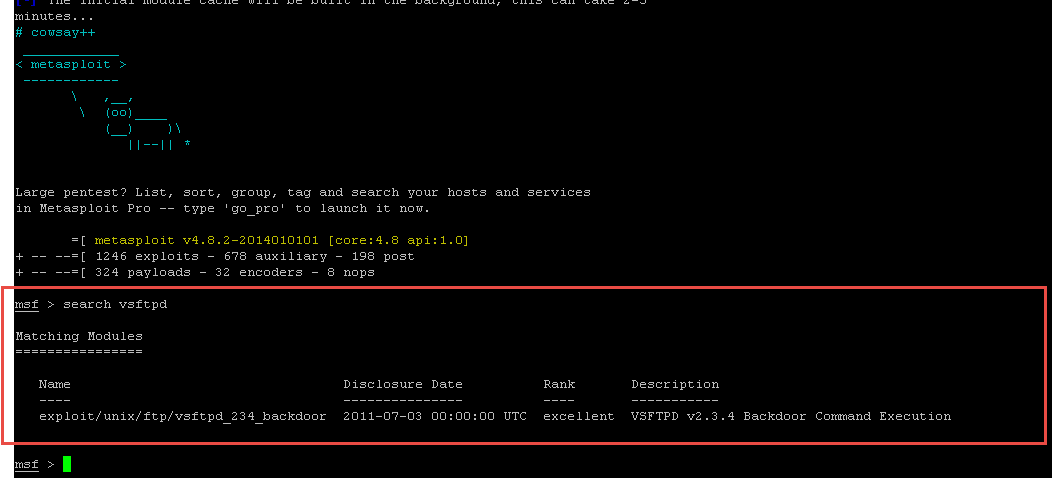


1. Search and exploit the vulnerability by using Metasploit

Once we find the vulnerability, we start our exploitation process by using Metasploit.



In this figure, we see that in order to make Metaploit works properly, we should firstly start postgresql database application. And, then we start the Metaploit for further hacking. In step 3 that is marked above, we use a console of Metaploit to execute some commands.



After we search the production in msfconsole, we find that this vulnerability’s first disclosure date is July 3th, 2011 and we also see that Metaploit mark this vulnerability as excellent which means that it is very serious. And, next, we use Metaploit explore it.

In the exploit, we first specify which vulnerability to use and then set the machines (target machine) which contains this vulnerability. After the settings are done, we simply type exploit command in step 3 and it start to exploit. In step 4, we can see that we have already successfully exploited the target, and I typed w to show current login users’ information.

1. Software vendors and patch download URL

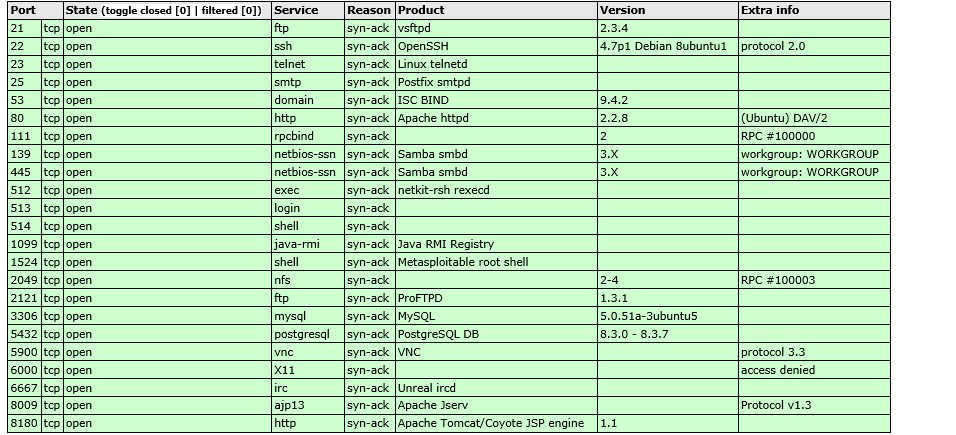
Vsftpd is a GPL licensed FTP server for Unix systems which is developed by Chris Evans, a contributor to GNU.

In order to solve the vulnerability, the only way can do is to patch Vsftpd and the patch download URL is list below.

<https://security.appspot.com/vsftpd.html>

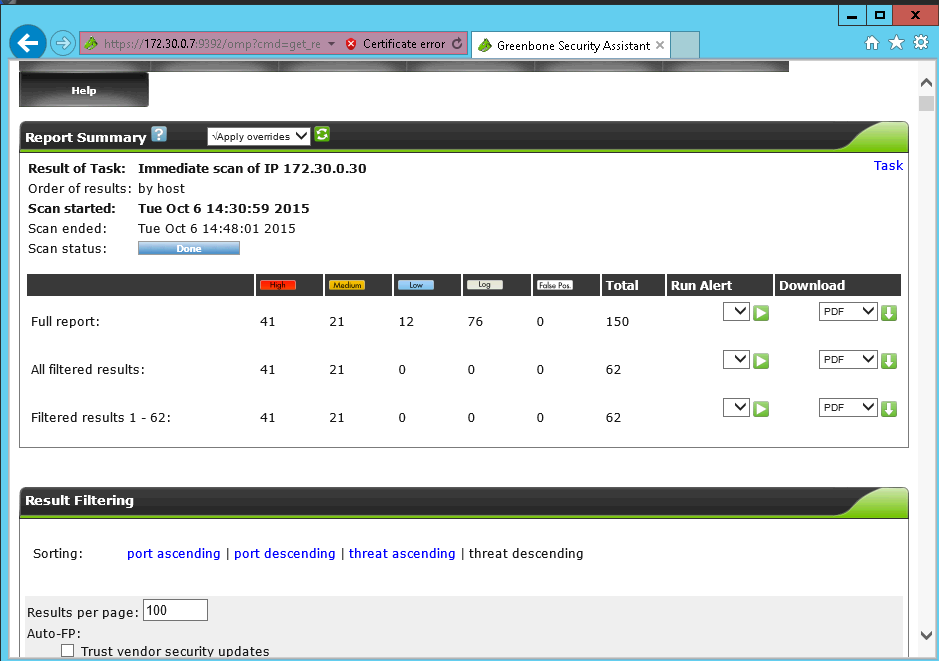
1. Report Screenshot
2. The number of open ports

In the intense scan report of 172.30.0.30, we have 23 open ports in total.

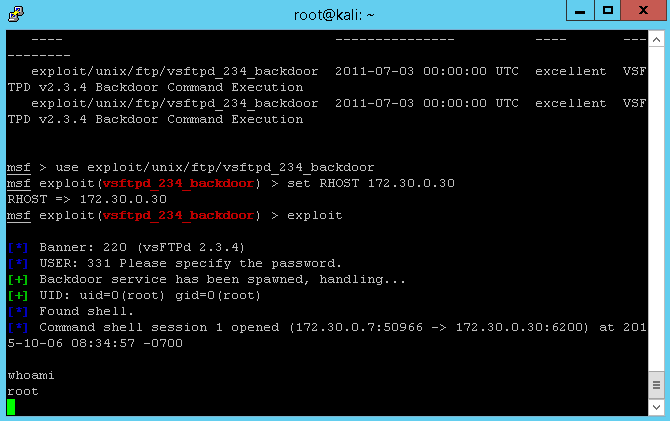


1. The number of High severity vulnerabilities

In the vulnerability scan result report of 172.30.0.30, we have 41 vulnerabilities marked as high.



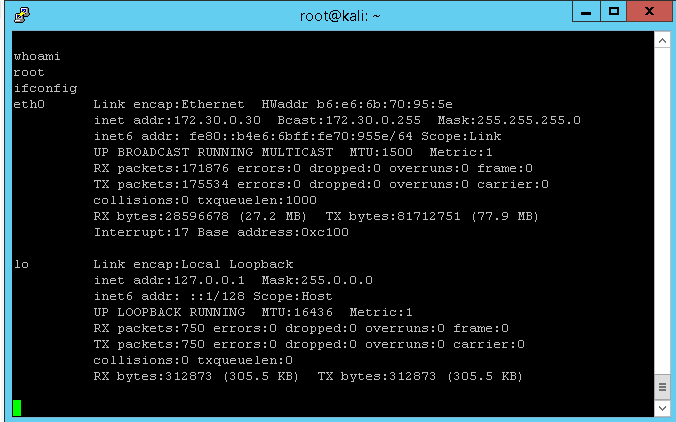
1. Whoami command that is executed from victim server



Explanation:

This figure shows that we successfully exploited the root privilege of target web server and we can execute arbitrary shell code in our target.

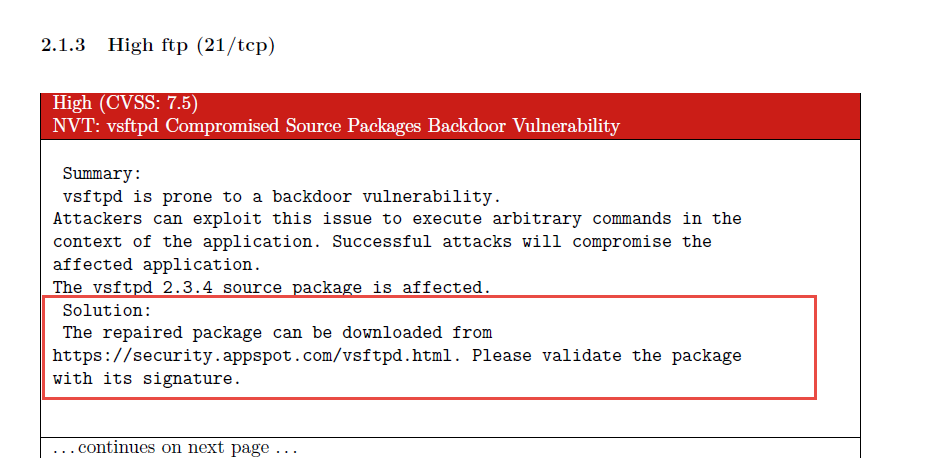
1. Ifconfig command that is executed from victim server



Explanation:

In this figure, it shows that we have already successfully exploited the vsftpd and get the root privilege which can run ifconfig command in the command line interface of target.

1. Recommend solutions for vsftpd



Explanation:

The solution to vsftpd is to patch your system with the latest package.

1. Other additional supporting text/image content