Penetration Test Report

by

James Barrington

Table of Contents

Executive Summary

As part of my Penetration testing and defense test I was asked to evaluate a given machine. The machine running was found to be vulnerable.

A total of 3 high vulnerabilities were discovered within the scope, with 3leading to {level of access/penetration}. I was able to escalate to root using an exploit. This essentially allowed me to do anything I wanted on the machine which poses a severe security risk.

I found 3 high vulnerabilities. With a unique count of 3

I found 2 medium-high vulnerabilities with a unique count of 4

Overall it is assessed that the Virtual machine tested represents a high security risk to the potential business operations of the machine. These risks relate to the possibility of a malicious party guessing passwords via brute force attempts allowing remote access to accounts, executing commands as the webserver remotely via shellshock or a reverse shell that is positioned via the ftp or the nfs.

To reduce the risk associated with the vulnerability, it is recommended that the owner of the Virtual Machine initiate a remediation program that covers the actions outlined in this report. The recommendations include, but are not constrained to

- Update the relevant kernal version
- Enforce a stronger password policy and access controls
- Review the privileges associated with the different user roles
- Remove any unnecessary services and resources

If the vulnerabilities outlined are addressed, then the attack surface will be greatly reduced and thus decreasing the likelihood of a successful attack.

PLANNING

Target IP: 172.16.97.154

The activities involved:

- Scanning and enumeration of services currently within the target scope
- Determination of possible vulnerabilities identified within services discovered

- Assessment and attempted exploitation of vulnerabilities, to eliminate false positive indications and penetrate the scoped network as much as possible
- Reporting of any identified penetrations, vulnerabilities, and recommended remediation advice

ENUMERATION

I scanned the Target IP for all tcp ports using zenmap (nmap).

This uncovered 11 open ports.

21 – vsftp 2.3.2

22 – open ssh 5.8

80 – apache 2.2.17

111 – rpcbind 2-4

2049 - nfs_acl

3306 -mysql

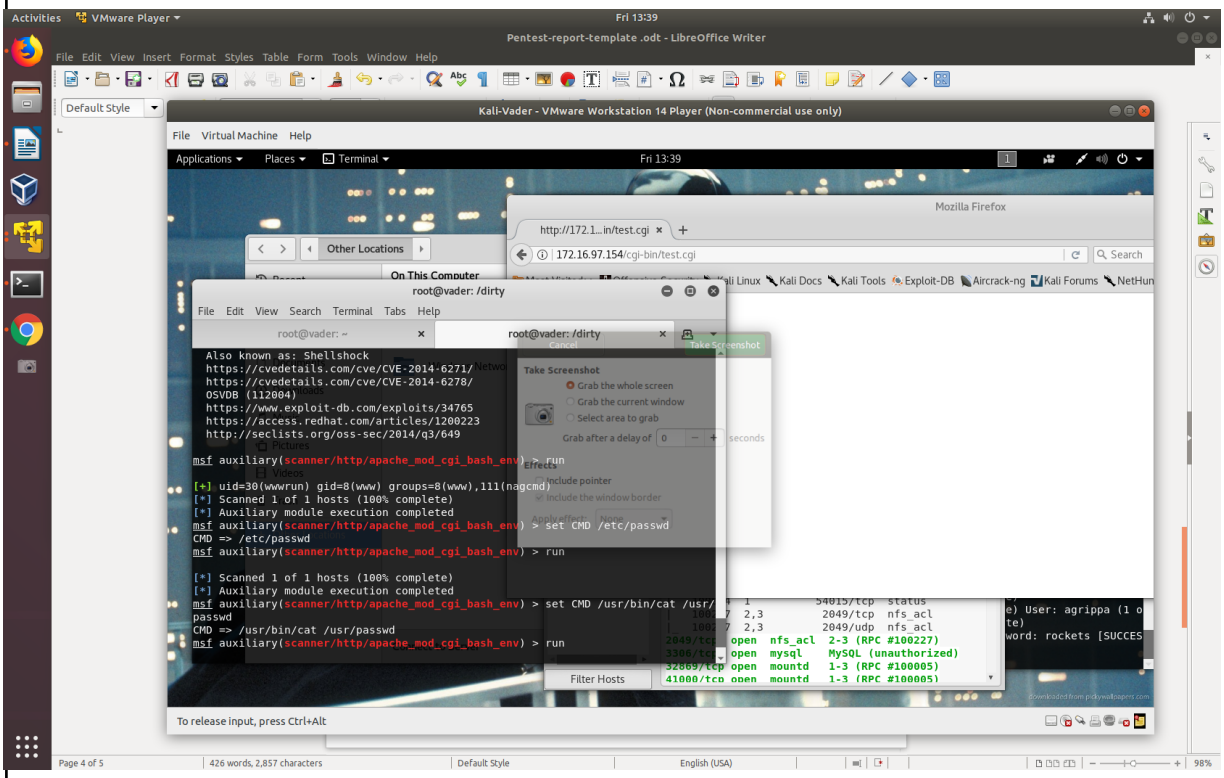
32689,41000,50678 – mountd

54015 – status

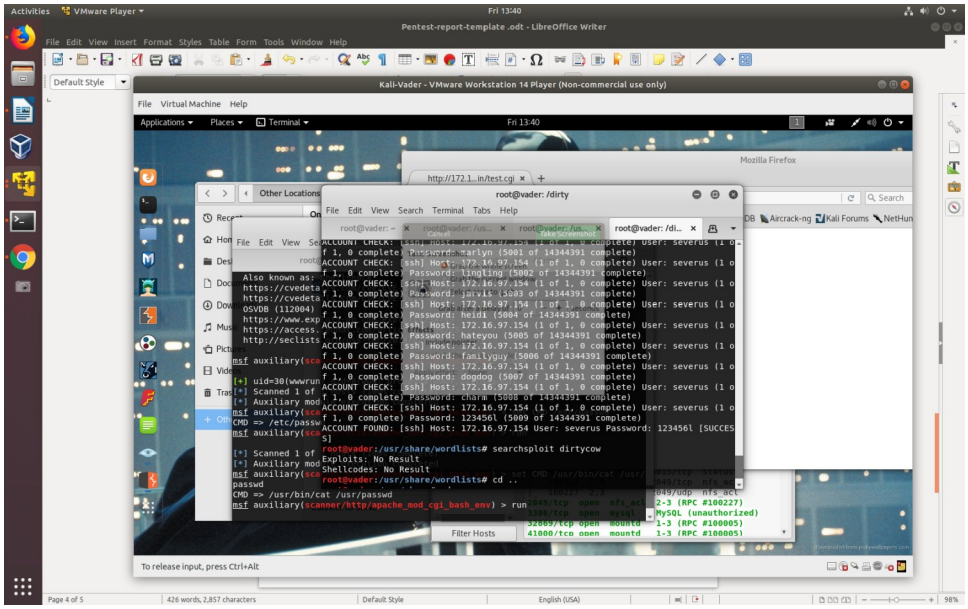
55441 - nlockmgr

ATTACK

First I checked the website which at first seemed to have nothing however in the source code of a file was a hint left by the admin. Because nmap return the kernal version when using the -A flag I knew the kernal version. The hint was the test.cgi was available still. Checking this out I realised this may provide a nice attack vector for shellshock. Using Metasploit I was able to confirm that the system was vulnerable to shellshock running the id command to verify.



We can remotely execute commands and easily start a netcat reverse shell if we were so inclined. Because there seems to be no use for the cgi-bin here it is safer to remove it all together and then you would not be required to update your kernal which could be more problematic.



The password for sevarus, julius and agrippa were easy to brute force. In order to stop this I would recommend implementing a stronger password policy by using the PAM tools or enforcing a stronger authentication method such as two factor authentication.

Doing this allowed me to use the severus account to access the base level flag

Flag 1 : base64 = dmluY2l0IHZlcml0YXMgc2VtcGVy

decoded = vincit veritas semperseverus

From here I noted the Kernal version using uname -r and found the following.

2.6.37.1-1.2-desktop

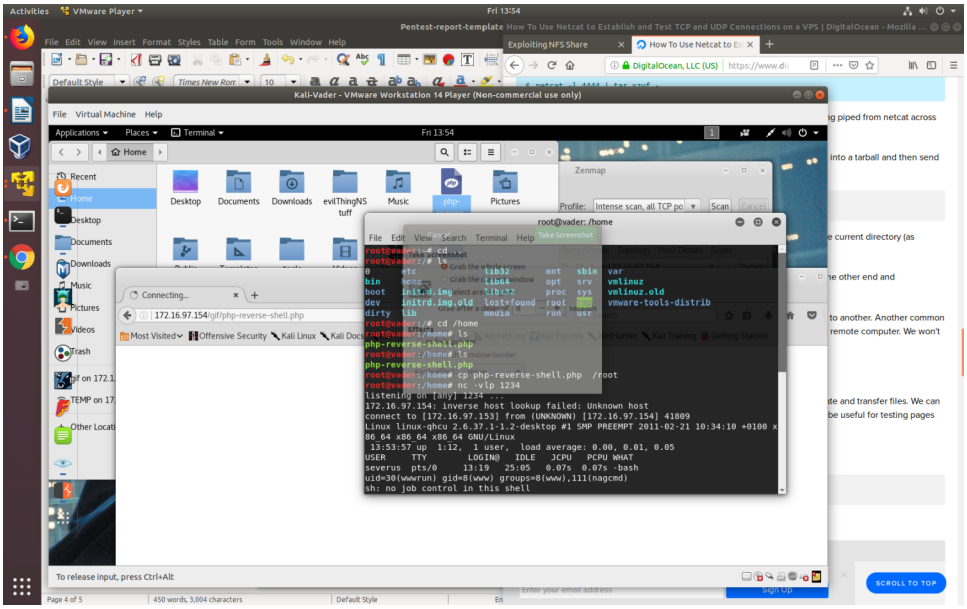
I was then able to elevate my privileges via a kernal exploit called dirty cow. I use scp to transfer the exploit I found using searchsploit and execute it locally. From here I was root and able to find flag 2

Flag 2 : base64 = bmloaWwgdGltb3I=

decoded = nihil timor

The shadow file has been overwritten at this point and should be reverted after use.

There are two publicly available NFS shares. One of these shares is the website. Using this as another attack vector I uploaded a php-reverse-shell and was able to start a reverse shell using the provided nfs. Allowing uploading of arbitrary files to the webserver is very bad and not recommended. I would remove the webserver nfs in order to remove this issue.



Next I checked the ftp server which allowed us to upload any files we wished anonymously. This could be used in conjunction with shellshock or other vulnerabilities that allow remote code execution. I uploaded a reverse shell to make sure it was possible and it was

DETAILED VULNERABILITY INFORMATION

For each vulnerability specify:

1 Shellshock CVE-2014-6271.

Description: Allows for remote command execution as the webserver.

Risk: This is a high risk vulnerability as it is internet facing and allows for remote command execution.

Solution: Update you kernal or remove the cgi-bin if it is not required

Assets Impacted: Any assets that are available to the web server may be potentially impacted including disclosure of arbitrary files and execution of malicious commands. This could also allow for a pivot inside the network to other machines or a priviledge escalation to root.

2 Password policy

Description: The passwords used for 3 of the 4 accounts was easily brute forceable via a dictionary attack using medusa with the dictionary from rockyou.

Risk: Password attacks are common place and a bad password is a high level risk.

Solution: Implement a strong password policy via PAM to do this you should set your dcredit and ucredit to at most -1 as well as implementing a password minimum length

Assets Impacted: The users could be impersonated and as such affect any assets they had access to or were involved with.

3 NFS shares

Description: Allows for anonymous remote file uploading to the webserver. This allowed us to run malicious php code as the webserver and start a php reverse shell.

Risk: This is a high risk.

Solution: Remove the ability to upload anything to the webserver anonymously. If possible remove it all together.

Assets impacted: Any assets that are available to the web server may be potentially impacted including disclosure of arbitrary files and execution of malicious commands. This could also allow for a pivot inside the network to other machines or a priviledge escalation to root.

4 Dirty Cow CVE-2016-5195

Description: This vulnerability exploits a race condition in the linux kernal that allows the attacker to overwrite any files without having the permission to do so. A common attack is to add a new super user to the shadow file with a password they specified.

Risk:This is a medium-high risk vulnerability. This attack requires local access and the ability to execute code.

Solution: You can update your kernal to a newer version that is not vulnerable or remove the ability to execute code from untrusted users.

Assets impacted: This exploit can corrupt arbitrary files in the operating system as well as provide an escalation method to any base level user. This could potentially impact the whole system and provide an easy pivot point to an attacker

5 Anonymous FTP uploaded

Description: Allows a potential attacker to upload a malicious file or just denial of service the ftp server.

Risk: This is a medium-high risk but can be very dangerous if used in association with other vulnerabilities that could allow the uploaded file to be executed

Solution: Deny access to anonymous users

Assets Impacted: Potential DOS to ftp and upload of malicious code resulting in a loss of access to the ftp.