

Penetration Test Report

Cantina Lorenzo VM

Table of Content

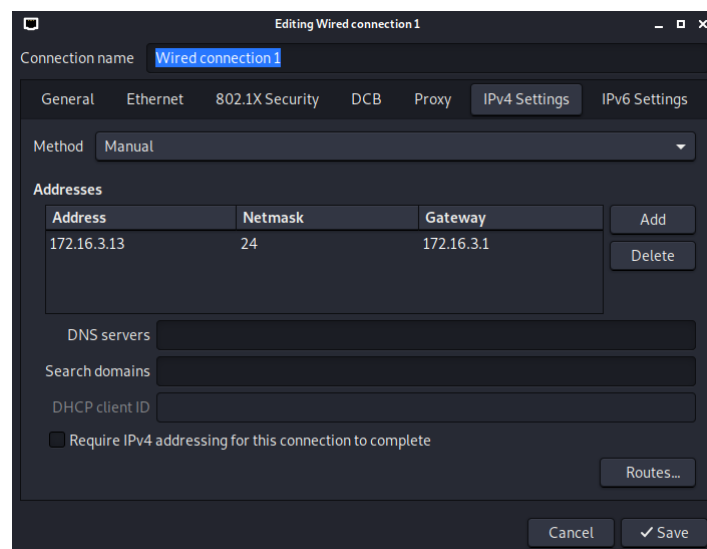
Executive Summary....	3
Vulnerabilities.....	3
Attack Scenarios.....	10
Conclusion.....	11

Executive Summary

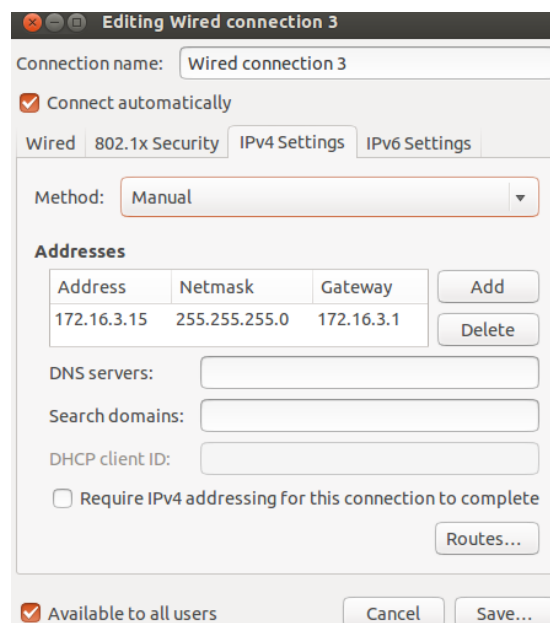
In this report, I will be analyzing Cantina Lorenzo VM, with the help of a Kali VM. I established the network connections for both VMs, after which I performed a ping test to test connectivity. Once everything was in place, I began my research on vulnerabilities that Cantina Lorenzo has. Using numerous tools, such as nmap, OpenVAS and Nessus I was able to come up with a list of vulnerabilities portrayed below. Every one of them carries a huge risk in breaching security and enables an attacker to gain access and exploit Cantina Lorenzo's files.

Vulnerabilities

In order to begin this task, establishing a connection between a Kali VM and Cantina Lorenzo's VM was needed. First, I have set up the network connection for the Kali VM, as shown below:



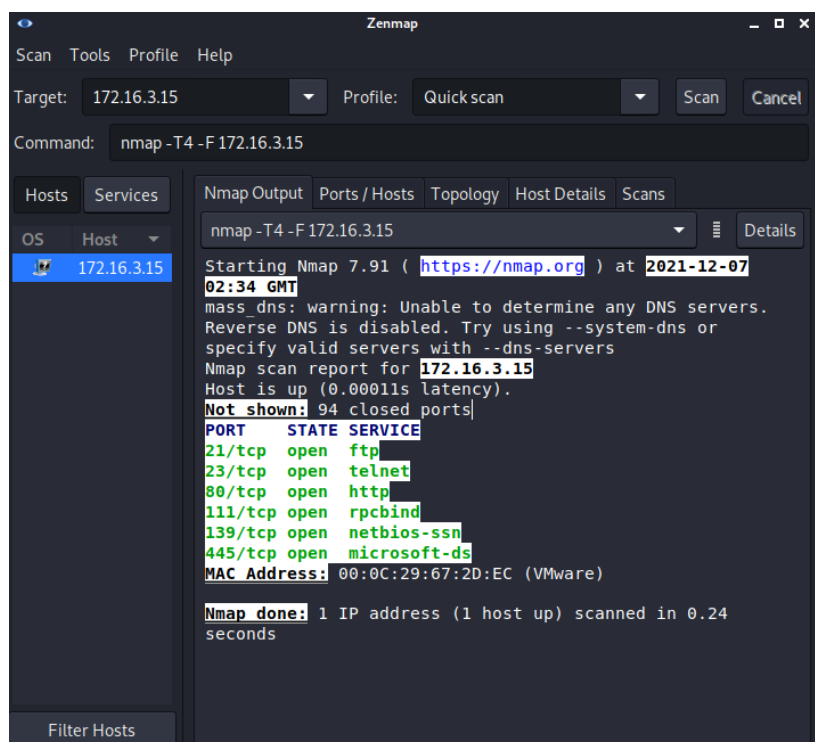
Right after Kali, I proceeded to set the network connection on Cantina Lorenzo's VM:



Once I restarted both machines, I proceeded to double check the connections I have set up by performing a ping from Kali to CL, which was successful:

```
(kali㉿kali)-[~]
$ ping 172.16.3.15
PING 172.16.3.15 (172.16.3.15) 56(84) bytes of data.
64 bytes from 172.16.3.15: icmp_seq=1 ttl=64 time=0.615 ms
64 bytes from 172.16.3.15: icmp_seq=2 ttl=64 time=0.324 ms
64 bytes from 172.16.3.15: icmp_seq=3 ttl=64 time=0.608 ms
64 bytes from 172.16.3.15: icmp_seq=4 ttl=64 time=0.898 ms
64 bytes from 172.16.3.15: icmp_seq=5 ttl=64 time=0.953 ms
64 bytes from 172.16.3.15: icmp_seq=6 ttl=64 time=0.923 ms
^Z
zsh: suspended ping 172.16.3.15
```

Once both connections were firmly established and beyond any reasonable doubt, I began my research on vulnerabilities of Cantina Lorenzo's VM. I opened the shell on the Kali VM and began my network mapper test, "nmap", which supplied me with the following results:



A vulnerability that is very easy to spot is the open port for file transfer protocol, which means an attacker would have access to stealing Cantina Lorenzo's files and/ or adding other new files, potentially containing malicious software, intended for bad purposes.

After nmap, I tried discovering any new vulnerabilities using OpenVAS. I proceeded to open the OpenVAS docker container from the Kali machine, updated it several times and then accesses localhost:8080 website. After running a scan on Cantina Lorenzo's VM, the result was the following:



Report: Tue, Dec 7, 2021 3:04 AM UTC

Done

ID: 1991a1cb-4d

Information	Results (5 of 145)	Hosts (1 of 1)	Ports (1 of 6)	Applications (3 of 3)	Operating Systems (1 of 1)	CVEs (2 of 2)	Closed CVEs (0 of 0)	TLS Certificates (0 of 0)	Error Me: (0 of 1)
-------------	-----------------------	-------------------	-------------------	--------------------------	-------------------------------	------------------	-------------------------	------------------------------	-----------------------

Vulnerability	Severity ▼	QoD	Host IP
Report outdated / end-of-life Scan Engine / Environment (local)	10.0 (High)	97 %	172.16.3.15
FTP Writeable Directories	10.0 (High)	80 %	172.16.3.15
Anonymous FTP Login Reporting	6.4 (Medium)	80 %	172.16.3.15
FTP Unencrypted Cleartext Login	4.8 (Medium)	70 %	172.16.3.15
TCP timestamps	2.6 (Low)	80 %	172.16.3.15

(Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity)

Again, the FTP writeable files show up, which confirms nmap results. This means the remote FTP server contains world-writeable files: /cgi-bin. This poses a serious threat to CL's VM, because an attacker could use this vulnerability to host data (this also includes illegal content!) on the FTP server.

Impact

An attacker may use this misconfiguration problem to use the remote FTP server to host arbitrary data, including possibly illegal content (ie: Divx movies, etc...).

There is also the fact that it was possible to login to the remote FTP service with anonymous accounts:

Detection Result

It was possible to login to the remote FTP service with the following anonymous account(s):

```
anonymous:anonymous@example.com
ftp:anonymous@example.com
```

Here are the contents of the remote FTP directory listing:

Account "anonymous":

```
-rw-r--r-- 1 0 0 3893 Aug 14 09:30 cantina.sql
drwxrwxrwx 2 0 0 4096 Aug 19 07:48 cgi-bin
-rw-r--r-- 1 0 0 133 Aug 14 09:42 db_config.php
-rw-r--r-- 1 0 0 3458 Aug 14 09:30 find.php
-rw-r--r-- 1 0 0 10571 Aug 14 09:30 functions.php
-rw-r--r-- 1 0 0 4377 Aug 14 09:30 home.php
drwxr-xr-x 2 0 0 4096 Aug 14 09:30 img
-rw-r--r-- 1 0 0 1814 Aug 14 09:30 index.php
-rw-r--r-- 1 0 0 1387 Aug 14 09:30 inv.php
-rw-r--r-- 1 0 0 969 Aug 14 09:30 licence-css.txt
-rw-r--r-- 1 0 0 34520 Aug 14 09:30 license-code.txt
-rw-r--r-- 1 0 0 4422 Aug 14 09:30 list.php
-rw-r--r-- 1 0 0 2073 Aug 14 09:30 mod.php
-rw-r--r-- 1 0 0 1532 Aug 14 09:30 print_inv.php
```

Account "ftp":

```
-rw-r--r-- 1 0 0 3893 Aug 14 09:30 cantina.sql
drwxrwxrwx 2 0 0 4096 Aug 19 07:48 cgi-bin
-rw-r--r-- 1 0 0 133 Aug 14 09:42 db_config.php
-rw-r--r-- 1 0 0 3458 Aug 14 09:30 find.php
-rw-r--r-- 1 0 0 10571 Aug 14 09:30 functions.php
-rw-r--r-- 1 0 0 4377 Aug 14 09:30 home.php
drwxr-xr-x 2 0 0 4096 Aug 14 09:30 img
-rw-r--r-- 1 0 0 1814 Aug 14 09:30 index.php
-rw-r--r-- 1 0 0 1387 Aug 14 09:30 inv.php
```

Knowing this, it is fair to state that an attacker who exploits the anonymous FTP login will gain access to files and upload and/or delete files.

Insight

A host that provides an FTP service may additionally provide Anonymous FTP access as well. Under this arrangement, users do not strictly need an account on the host. Instead the user typically enters 'anonymous' or 'ftp' when prompted for username. Although users are commonly asked to send their email address as their password, little to no verification is actually performed on the supplied data.

Remark: NIST don't see 'configuration issues' as software flaws so the referenced CVE has a severity of 0.0. The severity of this VT has been raised by Greenbone to still report a configuration issue on the target.

Detection Method

Details: [Anonymous FTP Login Reporting OID: 1.3.6.1.4.1.25623.1.0.900600](#)

Version used: 2021-10-20T09:03:29Z

Impact

Based on the files accessible via this anonymous FTP login and the permissions of this account an attacker might be able to:

- gain access to sensitive files
- upload or delete files.

Another discovery than can be considered an issue is the FTP Unencrypted Cleartext Login, which means CL's VM is running a file transfer protocol service that would allow cleartext login over unencrypted connections, therefore an attacker can uncover login names and passwords by sniffing traffic to the FTP service.

Summary

The remote host is running a FTP service that allows cleartext logins over unencrypted connections.

Detection Result

The remote FTP service accepts logins without a previous sent 'AUTH TLS' command. Response(s):

Non-anonymous sessions: 331 Please specify the password.

Anonymous sessions: 331 Please specify the password.

Detection Method

Tries to login to a non FTPS enabled FTP service without sending a 'AUTH TLS' command first and checks if the service is

Details: [FTP Unencrypted Cleartext Login OID: 1.3.6.1.4.1.25623.1.0.108528](#)

Version used: 2020-08-24T08:40:10Z


Impact

An attacker can uncover login names and passwords by sniffing traffic to the FTP service.

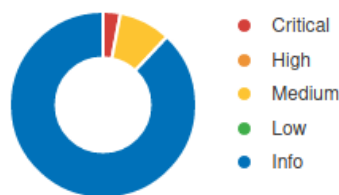
That wraps up OpenVAS, next tool I will be using is Nessus Essentials. I started Nessus from Kali's shell, accessed kali:8834 and after it compiled all the plugins, I performed an advanced scan on CL's machine, which revealed a few vulnerabilities:

<input type="checkbox"/>	Sev ▼	Name ▲	Family ▲	Count ▼	⚙
<input type="checkbox"/>	CRITICAL	Unix Operating System Unsupported Version Detection	General	1	🔄 ✎
<input type="checkbox"/>	MIXED	2 Microsoft Windows (Multiple Issues)	Windows	2	🔄 ✎
<input type="checkbox"/>	MEDIUM	SMB Signing not required	Misc.	1	🔄 ✎
<input type="checkbox"/>	MEDIUM	Unencrypted Telnet Server	Misc.	1	🔄 ✎

Scan Details

Policy: Advanced Scan
Status: Completed
Severity Base: CVSS v3.0 
Scanner: Local Scanner
Start: Today at 6:12 AM
End: Today at 6:14 AM
Elapsed: 3 minutes

Vulnerabilities



Some of the threats are related to using Telnet over an unencrypted channel, which is not recommended because logins, passwords and commands are transferred in cleartext. Anyone eavesdropping, a man-in-the-middle attacker can obtain these credentials and useful information, like stated earlier.

The biggest one is that the Unix operating system running on CL's machine is no longer supported. This means there's a compelling lack of support, which leads to no security patches being released for the product by the vendor.

CRITICAL Unix Operating System Unsupported Version Detection

Description

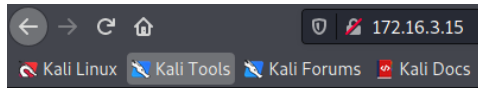
According to its self-reported version number, the Unix operating system running on the remote host is no longer supported.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.

An example of why this could be a problem is found in Windows. During a specific time frame, a ransomware was developed which infected PC's blocked all the user's files. To regain access to said files, the user had to pay the hijackers. To resolve this issue, Windows issued multiple security updates that patched the software and made it more secure, so users can enjoy a more risk-free environment.

Another concerning aspect is when I try to type in the browser Cantina Lorenzo's IP address. Once I click enter, the restaurant's site launches, without any login credentials required. This particularly poses a problem because an attacker doing the same thing would have access to inside information and all the content from the page is subject to modification, again, without any credentials required.

Up in the search bar, we can see the crossed out padlock, which indicates lack of security.



Cantina Lorenzo
GESTIONE CANTINA
Pagine

- [Riepilogo](#)
- [Carica/Scarica](#)
- [Inserisci/Cancella](#)
- [Inventario](#)
- [Cerca](#)

RIEPILOGO

Furthermore, there's access to CL's wine list, reservations and many other data that could be manipulated in bad faith by an attacker, as shown below.

LISTA VINI - COMPLETA

	Nome	VRBD
"	,print(chr(122).chr(97).chr(1	0 6 0 -6 1 V R B
'	;print(chr(122).chr(97).chr(1	0 0 0 0 1 V R B
:	:print(chr(122).chr(97).chr(11	0 0 0 0 1 V R B
@	@	0 0 0 0 1 V R B
\$	Set-cookie: Tamper=5624188a-8b	0 0 0 0 1 V R B
%	ZAP	0 0 0 0 1 V R B
&	ZAP %!1s%21s%31s%41s%51s%61s%7	0 0 0 0 1 V R B
*	ZAP*&cat /etc/passwd&*	0 0 0 0 1 V R B
^	ZAP^&sleep 156^	0 0 0 0 1 V R B
`	ZAP`&timeout /T 156`	0 0 0 0 1 V R B
~	ZAP~&type %SYSTEMROOT%\win.ini&	0 0 0 0 1 V R B

AGGIUNGI/RIMUOVI

[illegible]

RICERCA

Selezionare una ricerca per settimana, per mese o per anno

Numero settimana:

2021-49

Iniziale:

Mese:

12

/ 2021

Iniziale:


Anno:

2021

Iniziale:

After running the Advanced Scan Test on Nessus, I proceeded to try out another possible test, the Web Applications Test. This found a couple vulnerabilities; however one attracts my attention the most, specifically the CGI Generic SQL Injection.

Scan Details


Policy: Web Application Tests
Status: Completed
Severity Base: CVSS v3.0 
Scanner: Local Scanner
Start: Today at 6:20 AM
End: Today at 6:23 AM
Elapsed: 4 minutes

Vulnerabilities



web app / Plugin #11139

[Back to Vulnerabilities](#)

Hosts 1 Vulnerabilities 18 Notes 1 VPR Top Threats  History 1

HIGH CGI Generic SQL Injection

Description

By providing specially crafted parameters to CGIs, Nessus was able to get an error from the underlying database. This error suggests that the CGI is affected by a SQL injection vulnerability.

An attacker may exploit this flaw to bypass authentication, read confidential data, modify the remote database, or even take control of the remote operating system.

Solution

Modify the relevant CGIs so that they properly escape arguments.

~ ..

This SQL Injection poses a true web security issue, since it would give me the possibility to interfere with processes CL's apps make to the database. It would allow me to view and/ or retrieve data that are not normally supposed to be subject to these actions. I would be able to modify and/ or delete data and cause non-stop changes that would disrupt the normal workflow of CL. This flaw in security means an attacker with bad intents would try and bypass authentication and gain access to confidential data, manipulate remotely the database and eventually could even take control over the entire operating system. Ultimately, I would be able to escalate this SQL Injection Attack to compromise the VM and any other relevant back-end bits, or even come up with a "Denial of Service" type of attack.

Attack Scenarios

First attack

An immense vulnerability can be exploited when it comes to Cantina Lorenzo's database. All the important information CL has, is stored in a database, thus it's a really sweet spot for me to attack. The SQL injection vulnerability that OpenVAS was able to find, means I would be able to access the database and begin modifying certain parameters, figures and so on. Information like inventory, employee compensations, bonuses, invoices and many others would be subject to modification if I were to have access to them. For example, I could change an employee's compensation and they would receive much more than they were meant to, this way disbalancing CL's books. I would also be able to obtain employee information, like addresses, phone numbers, name, contacts everything, to devise a so called "Operation's Playbook" can be very easily finished with a swift, yet powerful SQL Injection Attack. Another attack I would be able to perform is modifying the inventory i.e. take the wine list which shows, presumably, the number of bottles of each type of wine. I could modify all the numbers, make them greater than they actually are and at some point, the database would show CL administrator that they have enough bottles of wine in storage (so there would be no need to order some more), they would open later on that day, and by the time they are half way through dinner service, they run out of wine. Telling a customer you cannot provide a glass of good red wine next to their veal steak would in some cases make them change their opinion on Cantina Lorenzo's service. A scenario like this could very easily have an impact on a much larger scale, for example modifying everything from the inventory and from here same principle applies. Either way, it has a huge potential to ruin Cantina Lorenzo's reputation, especially if there is a food critic dining the night my SQL Injection Attack impacted CL.

Second Attack

As a second potential attack on CL's VM, I will try to exploit the FTP vulnerability, which enables me to transfer files from client to server. By running nmap, I found that port 21 is open, which is a port exclusive to FTP. Anonymous login is allowed, so I can easily connect to the target IP and enter "anonymous" for username when it'll ask me to. Perfect, moving

right along. After finding a directory, the next logical step for me to take would be to replace the files contained in said folder with malicious ones, that could have legal implications. For example, after performing the first part of my penetration attack, it leaves an entire writeable and readable directory at my disposal. I would try to host data from Torrent type websites, like movies, music, software etc., so CL would play the role of a “seeder” a.k.a. uploader for these pirating websites. I could also plant evidence there of participating in a recent robbery, so CL’s administrator would have a very different relationship with the law. Arrests based on robbery evidence conducted at Cantina Lorenzo’s will also have a very strong impact from a marketing standpoint and personally, I would not like to eat at a “criminal’s” restaurant. There is also the possibility where I don’t find much in the first place, however I would use my initial access to start poking around and finding other bits of useful information, like when is the next maintenance (if any) going to take place. By brute forcing an administrator’s account, I could get access to admin privileges.

Third Attack

OpenVAS should me a vulnerability that particularly interests me. Specifically, the system has not been updated for years! To begin to understand why a couple small updates, done over the years which that at first glance don’t change a thing, are so important, let’s have a look at Microsoft. There was an outbreak of ransomware in 2017. Due to a back door that attackers found, they were able to come up with a software that sneaks into your systems, encrypts all your files and everything would be doomed. But, the hackers had the sole key to decrypting your files, meaning that you could not get the job done anywhere else. As most people, these hackers tried to make money, after hurting people, so for a certain amount (paid to them in Bitcoin, untraceable currency at the time) they would encrypt your files and you two would never see faces again. So, over the years, an attack of this kind might have been developed and Cantina Lorenzo’s VM is certainly exposed to it, without any recent updates, any new security patches and so on. A scenario that comes to mind would be taking place on a very busy Friday night, when Cantina Lorenzo cannot access their bookings, their inventory and would have no way of keeping track of all the income of that night. All this because I was able to sneak in a malware/ ransomware/ any kind of virus that disrupts normal workflow by exploiting security vulnerabilities that have been long known of, taken care of, but not when it comes to Cantina Lorenzo, since they lack all recent support. It would create an immense chaos among staff and it would also drop their morale, which would definitely hurt the business.

Conclusion

To sum up, the current state of Cantina Lorenzo’s VM shows it has many exploitable vulnerabilities. I began my research using nmap, OpenVAS and Nessus and all of them showed me exploitable security issues that could turn out to destroy Cantina Lorenzo. Simple things like an open FTP port, an OS that is not updated and SQL Injection are major flaws and constitute breaches in Cantina Lorenzo’s overall security. If exploited

independently (as shown in the 3 scenarios I managed to come up with), each vulnerability turned out to have an immense risk, however if all of them are combined- who knows what might happen. After tackling all the issues stated above, Cantina Lorenzo can achieve a very good level of security.