University of Salerno

Penetration Testing Report

VULNERABLE LAB DC - 5

Salvatore Froncillo | PTEH course | 12/01/2021

UNIVERSITÀ DEGLI STUDI DI SALERNO
DIPARTIMENTO DI INFORMATICA

Summary

1. Executive Summary

For this project relating to the Penetration Testing & Ethical Hacking exam, a Penetration Test activity was carried out, examining the DC-5 virtual machine.
This machine can be found from the official Vulhub website.
The aim of the testing was to analyze the security position of the target machine and suggest countermeasures for all the vulnerabilities found. A “Gray box” approach was used, in fact some basic information of the target machine and network structure was known.
The test was carried out from the point of view of an attacker with access to the local network, but who has no knowledge of the connected machines or the infrastructure.

Several low and high risk vulnerabilities have been found, which could cause service interruptions or even **full control of the machine by an attacker,** and it has been learned that adequate security countermeasures have not been implemented within the environment.

This report consists of a first part, in which we find the detailed analysis of the vulnerabilities detected during the engagement phase; and a second part consisting of the Remedation report, which highlights the solutions that could benefit the overall security of the infrastructure.

The level of risk present at the current state of the System is **HIGH.** Troubleshooting should be done **as soon as possible .** Once the remediations detailed below have been performed, the vulnerabilities illustrated will be
eliminated and the risk will return to acceptable levels.

2. Engagement Highlights

DC-5 is a vulnerable laboratory offered by the Vulnhub platform for educational purposes, so there are no limits on the methodologies and tools to be used to complete the process. For this reason, the inclusion of a non-disclosure agreement in the report would have been superfluous.

To carry out the safety test, the steps used for a Penetration Testing process were followed. After the first phase of Information Gathering, the following objectives were completed:

- Target IP address retrieval;
- Network scanning (Nmap);
- http services enumeration;
- Exploiting LFI vulnerability (Burpsuite);
- Reverse shell (netcat);
- Increase of privileges;
- Maintaining access via Backdoor (Metasploit - Msfvenom);

The following tools were used for the penetration testing process: Nmap, Burpsuite, Netcat, Metasploit, Msfvenom.

3. Vulnerability Report

Several vulnerabilities were found, the main ones concerning:

- A **medium critical vulnerability,** concerning the possibility of creating infinite loops in some processes by the attacker, with the possibility of decreasing computational resources and crashing some processes.
- 3 **highly critical** vulnerabilities , concerning respectively:
    - o An obsolete and vulnerable version of gnu screen for privilage escalation;
    - o An LFI-type web vulnerability, which allows an attacker to include malicious strings in the url;
    - o A vulnerability in the NGINX web server that allows attacks by DOS type.

Overall, these vulnerabilities, especially the highly critical one, raise the risk of compromise of the target machine by up to 80%.

4. Remediation Report

- **Correct** the vulnerabilities found.
- Constantly **update** the services used.
- **Implement** a whitelist to limit user input browsing the site web.
- Safety **checks** must be performed regularly.

5. Findings Summary

In this section, more detailed information about the target machine and its vulnerabilities will be presented. In the following chart, the vulnerabilities have been grouped by criticality:

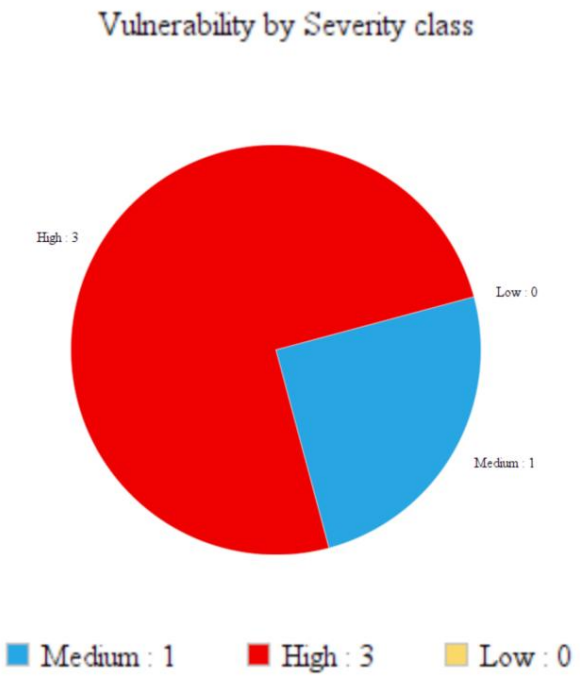

Figure 1 - Vulnerability pie chart

As already mentioned above, the Penetration Testing process involved only the host that has an IP address of 10.0.2.15.

The following table summarizes the identified vulnerabilities:

ID	vulnerability	Host criticality		Location
dc5-1	Local File Inclusion (LFI)	8	10.0.2.5	80 / tcp
dc5-2	Infinite loop on some processes	5.8	10.0.2.5	ngx_http_mp4_module
dc5-3	Gain root privileges	7.2	10.0.2.5	local
dc5-4	Denial of service	7.5	10.0.2.5	53 / udp

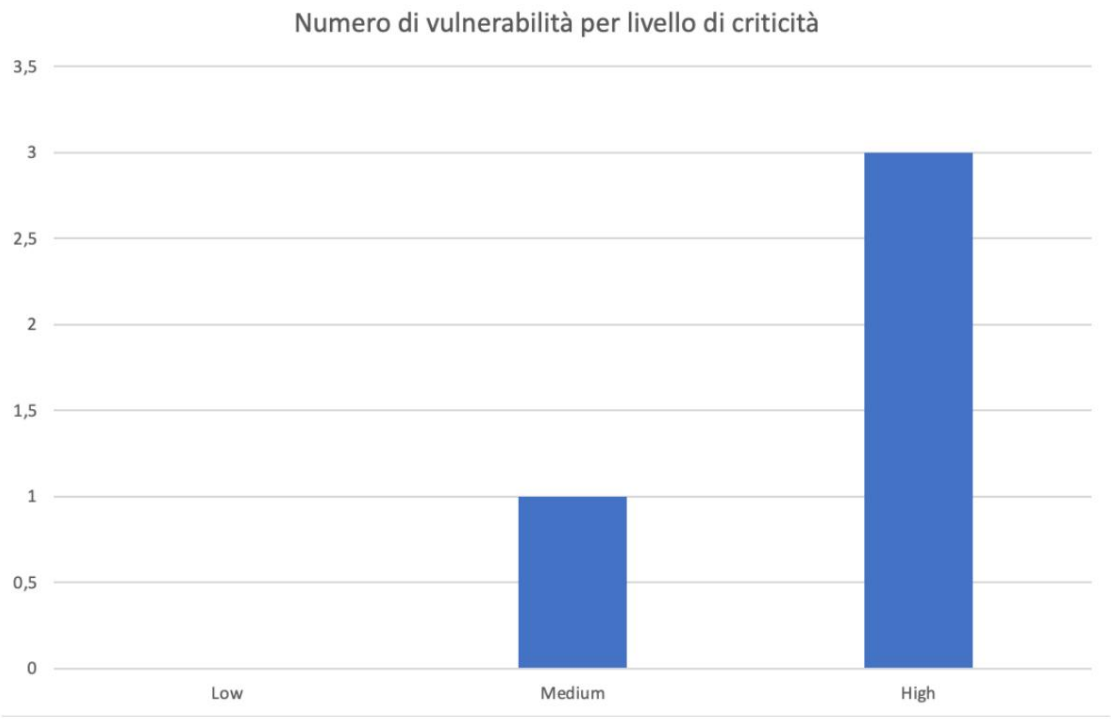

Figure 2 - Histogram of the number of vulnerabilities by level of criticality

6. Detailed Summary

In this section we will analyze the vulnerabilities in detail.

dc5-1: Local File Inclusion	
Critical issues	Tall
Description	LFI is a web vulnerability caused by mistakes made by a website or web application programmer.
Impact	An attacker can include malicious files that are subsequently executed by this website.
Recommendations	Implement a whitelist to limit user input.
Systems Involved	NGINX 1.6.2
References	https://www.acunetix.com/blog/articles/local-file-inclusion-lfi/

dc5-2: Infinite loop on some processes	
Critical issues	Medium
Description	Possibility of creating infinite loops on some processes by the attacker due to some malfunctioning modules.
Impact	Possibility of crashing a process or drastically reducing machine resources
Recommendations	Update NGINX to the latest version available.
Systems Involved	NGINX
References	https://ubuntu.com/security/notices/USN-3812-1

dc5-3: Gaining root privileges	
Critical issues	Tall
Description	GNU screen in versions prior to 4.5.1 allows local users to edit files
Impact	the attacker can gain root permissions.
Recommendations	Update the service.
Systems Involved	GNU screen and system
References	https://git.savannah.gnu.org/cgit/screen.git/tree/src/ChangeLog?h=v.4.5.1

dc5-4: Denial of service	
Critical issues	Tall
Description	NGINX versions prior to 1.9.10 allow remote DOS attacks
Impact	The service becomes unavailable
Recommendations	Update NGINX
Systems Involved	NGINX
References	https://access.redhat.com/errata/RHSA-2016:1425

7. References

• https://ubuntu.com/security/notices/USN-3812-1 • https://www.acunetix.com/blog/articles/local-file-inclusion-lfi/ • https://git.savannah.gnu.org/cgit/screen.git/tree/src/ChangeLog?h=v.4.5.1 • https://www.cvedetails.com/cve/CVE-2017-5618/ • https://access.redhat.com/errata/RHSA-2016:1425

8. Appendix