FINAL PROJECT

W12 D4

Fabio Belforti
DOC. Edoardo Castelli | Giuseppe Placanica

18 May 2025

PAIRING THE 2 NESSUS'S SCAN

192.168.51.100

CRITICAL	HIGH	MEDIUM	LOW	INFO
56	6	25	8	127

Scan Information

Start time:	Fri May 16 13:14:22 2025
End time:	Fri May 16 13:36:36 2025

Host Information

Netbios Name:	METASPLOITABLE
IP:	192.168.51.100
MAC Address:	D2:49:AB:A9:48:F1
OS:	Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

AFTER REMEDIATIONS

192.168.51.100

CRITICAL	HIGH	MEDIUM	LOW	INFO
41	5	25	8	106

Scan Information

Start time:	Sun May 18 12:06:29 2025
End time:	Sun May 18 12:29:26 2025

Host Information

Netbios Name:	METASPLOITABLE
IP:	192.168.51.100
MAC Address:	D2:49:AB:A9:48:F1
OS:	Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

CONCLUSION

Throughout this lab, I learned the importance of systematically analyzing vulnerabilities and applying targeted remediation strategies. Tools like Nessus provide a comprehensive overview of exposed services and known vulnerabilities, allowing security teams to effectively prioritize remediation based on severity.

One key takeaway was understanding how seemingly small changes—such as configuring authentication for VNC or disabling unnecessary services—can significantly reduce a system's attack surface. Repeating the scan after applying fixes proved essential to verify the effectiveness of the remediation steps and to ensure that no new vulnerabilities were introduced in the process.

Security is not a one-time task, but an ongoing effort that requires continuous monitoring, testing, and improvement. While not all issues were resolved during this session, the noticeable reduction in critical vulnerabilities demonstrates the impact of even basic remediation actions. Further hardening and detailed configuration reviews are recommended to achieve a more robust security posture.

The table below summarizes the vulnerabilities identified during the scans, along with their corresponding remediation status.

Vulnerability	Type	Status After Remediation	Notes
Apache Log4Shell CVE-2021-45046	Remote Code Execution (RCE)	Reduced from 25 to 3	Remediation performed on port 111
Apache Log4Shell RCE detection via callback	Remote Code Execution (FTP callback)	Resolved	Monitor for further activity
Apache Tomcat AJP Connector Request Injection (Ghostcat)	Injection vulnerability on AJP connector	Resolved	Configuration update needed
SSL Medium Strength Cipher Suites Supported (SWEET32)	Weak encryption	Resolved	Disable weak cipher suites
VNC Server 'password' Password	Vnc weak password	Resolved	Created a safe password for VNC connections

THANKS FOR YOUR ATTENTION

Fabio Belforti

Stud. Cybersecurity Analyst

EPICODE

18/05/2025