Penetration Testing Report: SMTP Service Enumeration on Port 5000

Target: 10.137.0.149

Test Conducted By: MD SAMSUL KABIR

Date:21/09/2024

Test Scope: Authorized penetration testing on the port 5000.

Summary:

An assessment of the UPnP service running on port 5000 was conducted to identify potential vulnerabilities. Various scanning tools, including Nmap and Metasploit Framework, were utilized to enumerate services and attempt exploitation.

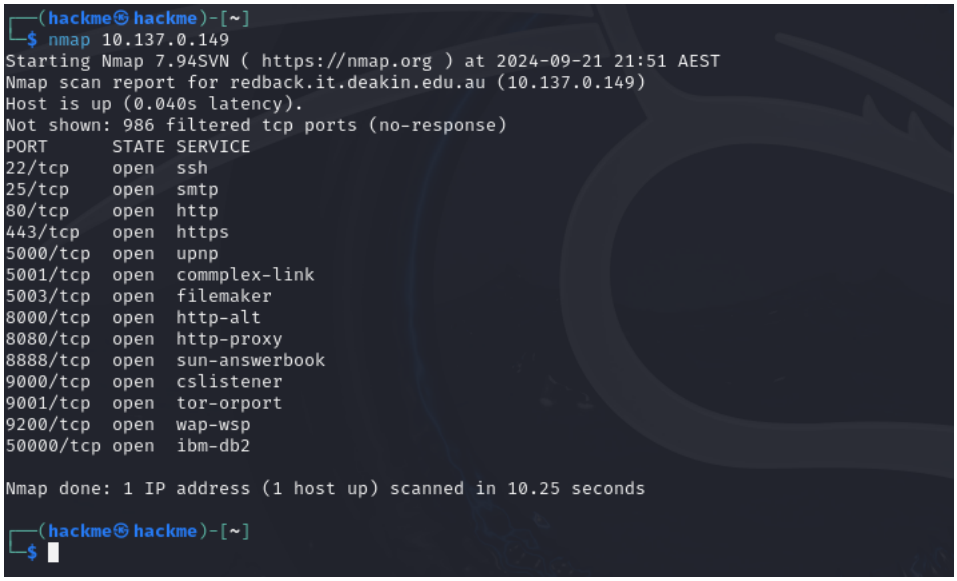
Findings:

Port: 5000/tcp

Service: UPnP

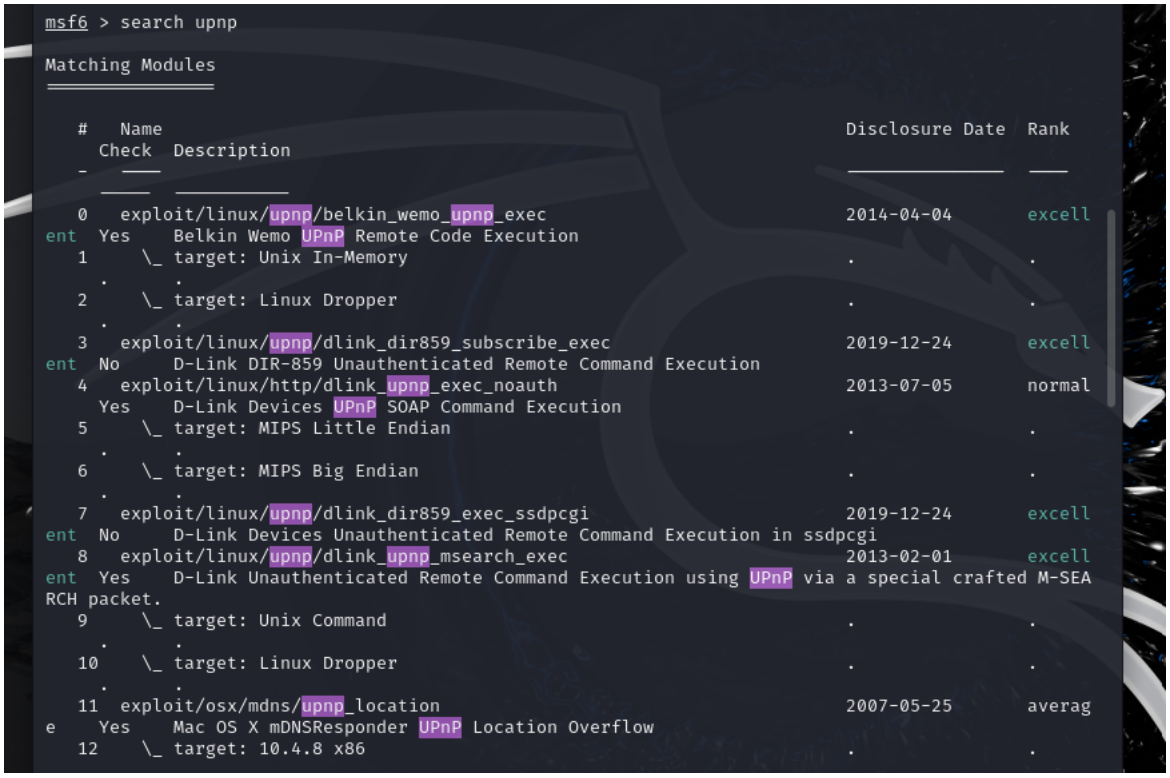
State: Filtered

First to check the open ports we use “nmap 10.137.0.149”.

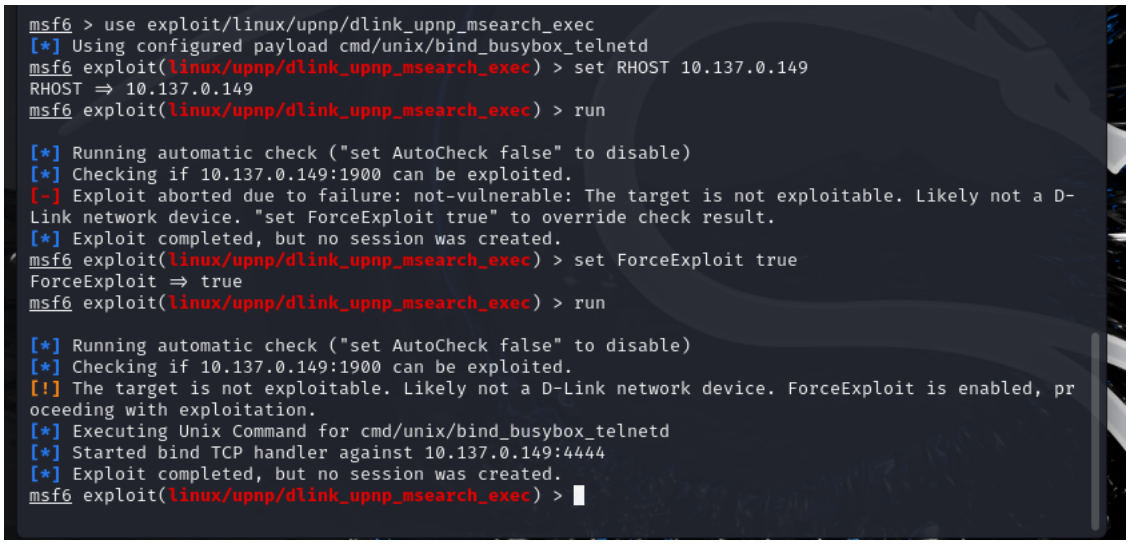


Now to further investigate the SSH service to identify the version running on the target. we will use "nmap -sV -p 5000 10.137.0.149".This will help in determining whether there are any known vulnerabilities associated with that particular version.

Exploitation on msfconsole



Scripts for upnp



Exploit unsuccessful

Nmap scan indicated that the UPnP service is running on the target, but the port was filtered, preventing detailed examination of the service's version or configurations.

Exploit Attempts:

Various UPnP-related exploits were assessed, specifically targeting D-Link devices.

Attempts to exploit the D-Link UPnP Remote Command Execution vulnerability were made; however, the target was determined to be non-exploitable.

Exploit Details:

Used exploit: exploit/linux/upnp/dlink_upnp_msearch_exec

Despite enabling ForceExploit, no session was created, indicating the target does not meet the exploit's requirements.

Potential Risks

The inability to exploit the UPnP service suggests that while the service is exposed, it may not be configured in a vulnerable manner. However, the following risks remain:

Filtered Ports: The filtering on port 5000 may indicate security measures in place, but it could also lead to false security perceptions.

Misconfigurations: If misconfigurations exist within the UPnP service, they could be exploited in future assessments.

Exposure of UPnP Services: UPnP services are known for vulnerabilities, and the presence of such services on a network can increase the attack surface.

Recommendations

Service Hardening:

Disable UPnP if not needed, as it introduces unnecessary risks.

Regularly review and update service configurations to minimize potential vulnerabilities.

Network Segmentation:

Segment networks to limit exposure to UPnP services, ensuring that only trusted devices can access them.

Monitoring and Logging:

Implement monitoring for unusual activities on UPnP services and other network services.

Regularly review logs for any unauthorized access attempts or anomalies.

Regular Penetration Testing:

Conduct periodic penetration testing to identify new vulnerabilities or changes in the attack surface.

Conclusion

The assessment of the UPnP service on the target indicated potential exposure but no current vulnerabilities exploitable with the tested methods. Continuous monitoring, service hardening, and regular testing are recommended to maintain a secure environment.