Pentest report - 192.168.111.137

Summary

I. Overview

II. DNS Request

III. Data about HTTP/HTTPS certificate

IV. NMAP scan

V. Nikto scan

VI. Potential vulnerabilities

VII. Exploit find

VIII. Recommendations

I. Overview

This report presents the results of a vulnerability assessment conducted on **192.168.111.137** using Python modules. The objective of this assessment is to provide a brief overview of the security posture of the target and identify potential vulnerabilities that could be exploited by attackers.
The main objective of the assessment was to identify vulnerabilities that could be used by attackers to compromise the confidentiality, integrity, or availability of the target. Python modules are used to automate the scanning process and identify potential vulnerabilities in the target.
Date: 2024-05-09 14:58
Target : 192.168.111.137
Type: vulnerability scanner

II. DNS Request

Check your domain name or the API website (https://networkcalc.com/api/)

III. Data about HTTP/HTTPS certificate

Error. Check your domain name or the API website (https://networkcalc.com/api/)

IV. NMAP scan

Port	Service	Version
21	ftp	2.3.4
22	ssh	4.7p1 Debian 8ubuntu1
23	telnet	
25	smtp	
53	domain	9.4.2
80	http	2.2.8
111	rpcbind	2
139	netbios-ssn	3.X - 4.X
445	netbios-ssn	3.X - 4.X
512	exec	

Port	Service	Version
513	login	
514	tcpwrapped	
1099	java-rmi	
1524	bindshell	
2049	nfs	2-4
2121	ftp	1.3.1
3306	mysql	5.0.51a-3ubuntu5
5432	postgresql	8.3.0 - 8.3.7
5900	vnc	
6000	X11	
6667	irc	
8009	ajp13	
8180	http	1.1

V. Nikto scan

Web server : Apache/2.2.8 (Ubuntu) DAV/2
Server uses : PHP/5.2.4-2ubuntu5.10
The server doesn't support compression.
Version of software might be found in the following header Server : 2.2.8
Version of software might be found in the following header X-Powered-By : 5.2.4
Target URL don't use any redirection
Target URL isn't protected by a basic HTTP authentication
The anti-clickjacking X-Frame-Options header is not present.

The X-XSS-Protection header is not defined.
The X-Content-Type-Options header is not set.

VI. Potential vulnerabilities

CVE ID	Description	Score
CVE-2011-2523	vsftpd 2.3.4 downloaded between 20110630 and 20110703 contains a backdoor which opens a shell on port 6200/tcp.	9.8
CVE-2011-1013	Integer signedness error in the drm_modeset_ctl function in (1) drivers/gpu/drm/drm_irq.c in the Direct Rendering Manager (DRM) subsystem in the Linux kernel before 2.6.38 and (2) sys/dev/pci/drm/drm_irq.c in the kernel in OpenBSD before 4.9 allows local users to trigger out-of-bounds write operations, and consequently cause a denial of service (system crash) or possibly have unspecified other impact, via a crafted num_crtcs (aka vb_num) structure member in an ioctl argument.	
CVE-2012-1577	lib/libc/stdlib/random.c in OpenBSD returns 0 when seeded with 0.	9.8
CVE-2010-4478	OpenSSH 5.6 and earlier, when J-PAKE is enabled, does not properly validate the public parameters in the J-PAKE protocol, which allows remote attackers to bypass the need for knowledge of the shared secret, and successfully authenticate, by sending crafted values in each round of the protocol, a related issue to CVE-2010-4252.	
CVE-2015-8461	Race condition in resolver.c in named in ISC BIND 9.9.8 before 9.9.8-P2 and 9.10.3 before 9.10.3-P2 allows remote attackers to cause a	

CVE ID	Description	Score
	denial of service (INSIST assertion failure and daemon exit) via unspecified vectors.	
CVE-2017-3141	Failed to fetch CVE details	
CVE-2012-5166	Failed to fetch CVE details	
CVE-2008-4163	Failed to fetch CVE details	
CVE-2012-3817	Failed to fetch CVE details	
CVE-2008-0122	Failed to fetch CVE details	
CVE-2012-1667	Failed to fetch CVE details	
CVE-2010-0382	Failed to fetch CVE details	
CVE-2012-4244	Failed to fetch CVE details	
CVE-2014-8500	Failed to fetch CVE details	
CVE-2011-3192	Failed to fetch CVE details	
CVE-2017-3167	Failed to fetch CVE details	
CVE-2009-1891	Failed to fetch CVE details	
CVE-2017-7679	Failed to fetch CVE details	
CVE-2009-1890	Failed to fetch CVE details	
CVE-2017-7494	Failed to fetch CVE details	
CVE-2020-1472	Failed to fetch CVE details	
CVE-2022-4514	Failed to fetch CVE details	
CVE-2020-2571	Failed to fetch CVE details	
CVE-2020-1074	Failed to fetch CVE details	
CVE-2020-1704	Failed to fetch CVE details	
CVE-2017-7494	Failed to fetch CVE details	

CVE ID	Description	Score
CVE-2020-1472	Failed to fetch CVE details	
CVE-2022-4514	Failed to fetch CVE details	
CVE-2020-2571	Failed to fetch CVE details	
CVE-2020-1074	Failed to fetch CVE details	
CVE-2020-1704	Failed to fetch CVE details	
CVE-2010-3867	Failed to fetch CVE details	
CVE-2019-1281	Failed to fetch CVE details	
CVE-2011-4130	Failed to fetch CVE details	
CVE-2009-0542	Failed to fetch CVE details	
CVE-2009-2446	Failed to fetch CVE details	
CVE-2008-0226	Failed to fetch CVE details	
CVE-2009-4484	Failed to fetch CVE details	
CVE-2013-1903	Failed to fetch CVE details	
CVE-2013-1902	Failed to fetch CVE details	
CVE-2019-1016	Failed to fetch CVE details	
CVE-2013-1900	Failed to fetch CVE details	
CVE-2010-1169	Failed to fetch CVE details	
CVE-2015-3166	Failed to fetch CVE details	
CVE-2015-0244	Failed to fetch CVE details	
CVE-2010-1447	Failed to fetch CVE details	

VII. Exploit find

Exploits found for CVE-2017-3141:

Exploit Title	Path
Exploit Title	Path
BIND 9.10.5 - Unquoted Service Path Privilege Escalation	windows/local/42121.txt

Exploits found for CVE-2020-1472:

Exploit Title	Path
Exploit Title	Path
ZeroLogon - Netlogon Elevation of Privilege	windows/remote/49071.py

Exploits found for CVE-2009-4484:

Exploit Title	Path
Exploit Title	Path
MySQL - yaSSL CertDecoder::GetName Buffer Overflow (Metasploit)	linux/remote/16850.rb

Exploits found for CVE-2011-3192:

Exploit Title	Path
Exploit Title	Path
Apache - Denial of Service	linux/dos/18221.c
Apache - Remote Memory Exhaustion (Denial of Service)	multiple/dos/17696.pl

Exploits found for CVE-2017-7494:

Exploit Title	Path
Exploit Title	Path
Samba 3.5.0 - Remote Code Execution	linux/remote/42060.py
Samba 3.5.0 < 4.4.14/4.5.10/4.6.4 - 'is_known_pipename()' Arbitrary	linux/remote/42084.rb

Exploits found for CVE-2009-0542:

Exploit Title	Path
Exploit Title	Path
ProFTPd - 'mod_mysql' Authentication Bypass	multiple/remote/8037.txt
ProFTPd 1.3 - 'mod_sql' 'Username' SQL Injection	multiple/remote/32798.pl

Exploits found for CVE-2011-2523:

Exploit Title	Path
Exploit Title	Path
vsftpd 2.3.4 - Backdoor Command Execution	unix/remote/49757.py
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)	unix/remote/17491.rb

Exploits found for CVE-2008-0226:

Exploit Title	Path
Exploit Title	Path

MySQL 6.0 yaSSL 1.7.5 - Hello Message Buffer Overflow (Metasploit)	linux/remote/9953.rb
MySQL yaSSL (Linux) - SSL Hello Message Buffer Overflow (Metasploit)	linux/remote/16849.rb
MySQL yaSSL (Windows) - SSL Hello Message Buffer Overflow (Metasploi	windows/remote/16701.rb

Exploits found for CVE-2009-2446:

Exploit Title	Path
Exploit Title	Path
MySQL 5.0.75 - 'sql_parse.cc' Multiple Format String Vulnerabilities	linux/dos/33077.c

VIII. Recommendations

Keep your systems up-to-date with the latest security patches and updates for all software and services running on your domain or IP address. Vulnerabilities are often discovered and patched by vendors, so it's important to stay current with updates to minimize risk.
We also recommend reviewing the list of links provided in this report, which point to known exploits and vulnerabilities affecting various services. These links can provide additional information and guidance on how to mitigate these specific security risks for your domain or IP address.
By following these recommendations and staying vigilant against emerging security threats, you can help protect your systems and data from unauthorized access and exploitation.