PENTEST BD

Penetration Testing Report of CC Commerce

Version: 1.0

Prepared By

Rishad Istiak

Pentest BD

Presented To:

Mr. John

CC Commerce

Date: 5 May 2022

PENTEST BD

Table of Contents

PENTEST BD

EXECUTIVE SUMMARY

Pentest BD has conducted a comprehensive penetration test of CC Commerce to identify the vulnerabilities in their network & web application. The time period of this assessment is from 10 January 2022 to 5 April 2022.

Test Scope

In this engagement, one network and one web application of CC Commerce was in scope for testing. No Denial of Service and Social Engineering attacks were permitted. The assessment was performed using various industry standard tools like nmap, nessus, burpsuite, metasploit etc.

Testing Summary

Pentest BD has tested all the IP addresses and web applications and evaluated the security posture of CC Commerce. Different attacks like default credential, misconfiguration, broken access control, backdoor etc are tested.

Recommendations

Based on the detected vulnerabilities, Pentest BD is providing the following recommendations to enhance the overall security posture of CC Commerce.

- ✓ Disable unused accounts
- ✓ Enforce proper password policy
- ✓ Enable authentication for the services
- ✓ Enable auto update feature

PENTEST BD

TESTING APPROACH

Overview

The whole assessment was performed in several phases. The following phases has been used in this penetration testing engagement.

1. **Planning:** Rules of engagement, scopes, goals etc. are defined in this phase.
2. **Discovery:** In this phase, scanning is performed to identify potential vulnerabilities.
3. **Attack:** Try to exploit the vulnerabilities to identify potential vulnerabilities.
4. **Reporting:** All the findings & evidences are properly documented in this phase.

Fig: Penetration Testing Methodology

INTERNAL NETWORK FINDINGS

Scope

For internal assessment, the following IP addresses are in scope.

Target IP Addresses
192.168.179.128

PENTEST BD

192.168.179.142

Services by Host and by Port

In the discovery phase, Pentest BD has performed scanning with nmap to find out the open ports and services for the in scope IP addresses. Each IP address was tested for both TCP & UDP ports. The ports & services that are exploitable has been highlighted.

IP Address	TCP/UDP	PORT	SERVICE	VERSION
192.168.179.128	TCP	21	ftp	vsftpd 2.3.4
	TCP	22	ssh	OpenSSH 4.7p1 Debian 8ubuntu1
	TCP	445	netbios-ssn	Samba smbd 3.X - 4.X
	TCP	1524	bindshell	root shell
	TCP	2121	ftp	ProFTPD 1.3.1
	TCP	6667	irc	UnrealIRCd
192.168.179.142	TCP	21	ftp	ProFTPD 1.3.1
	TCP	22	ssh	OpenSSH 4.7p1 Debian 8ubuntu1
	TCP	25	smtp	Postfix smtpd
	TCP	3306	mysql	MySQL 5.0.96-0ubuntu3
	TCP	3632	distccd	distccd v1
	TCP	5901	vnc	VNC (protocol 3.8)

PENTEST BD

Vulnerability Summary & Report

4	1	2	0	0
Critical	**High**	**Medium**	**Low**	**Informational**

Vulnerability Name	Severity	Recommendation
IPT-01: Backdoor Command Execution	Critical	Upgrade the service
IPT-02: Default Credential In SSH	HIGH	Use complex password
IPT-03: Unauthenticated SMB Share Access	MEDIUM	Enable authentication
IPT-04: Bind Shell Backdoor Detection	CRITICAL	Remove bind shell
IPT-05: UnrealIRCD Backdoor Detection	CRITICAL	Remove backdoor
IPT-06: Distcc Deamon Command Execution	CRITICAL	Disable the service
IPT-07: Weak Password In VNC	MEDIUM	Change password

Vulnerability Details

IPT-01: Backdoor Command Execution	
Location	192.168.179.128:21

Description	The target host has ftp enabled. The ftp version is vsftpd 2.3.4. This version is vulnerable to backdoor command execution. A metasploit module is successfully used to exploit the system and gain command execution
Impact	CRITICAL
Remediation	Upgrade the Vsftpd service to the latest one.

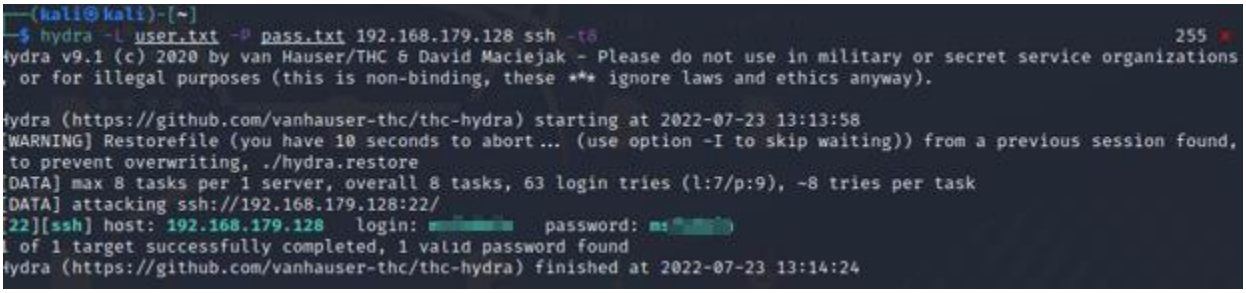
Evidence

References

- Reference line 1
- Reference line 2

IPT-02: Default Credential In SSH	
Location	192.168.179.128:22
Description	The target host has SSH service enabled. SSH is used for secure remote access. A Password cracking tool hydra has been used to check if the target is using default credential & we have found that the target is using default credential.
Impact	HIGH
Remediation	Change the default credentials & disable the unused accounts. Also apply a proper password policy.

Evidence

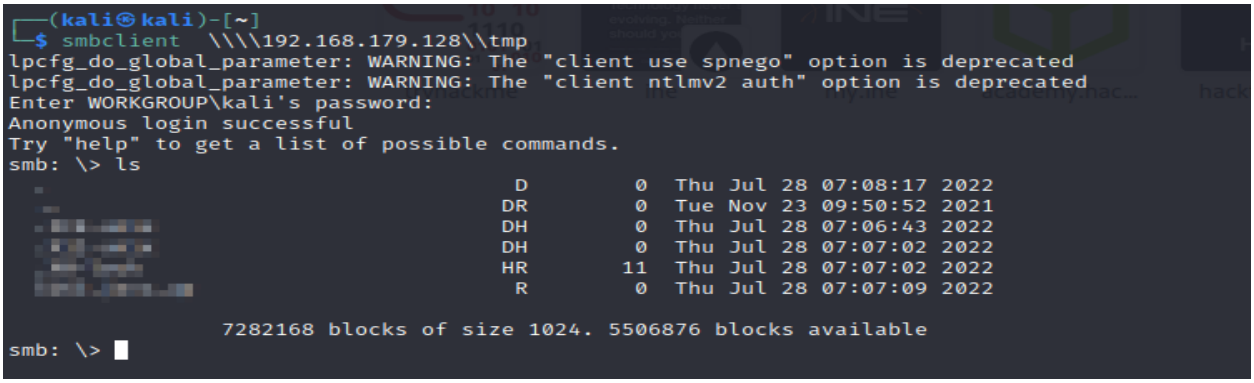


References

- Reference line 1
- Reference line 2

IPT-03: Unauthenticated SMB Share Access	
Location	192.168.179.128:445
Description	The target host has File share service enabled. But it doesn't require any authentication mechanism to access the shares.
Impact	MEDIUM
Remediation	Disable SMB service. If SMB is enabled, make sure to apply authentication mechanism to access the shares.

Evidence



PENTEST BD

References

- Reference line 1
- Reference line 2

IPT-04: Bind Shell Backdoor Detection	
Location	192.168.179.128:1524
Description	A shell is listening on the remote port 1524 without any sort of authentication required. An attacker can use it by connecting to the remote port and sending commands directly
Impact	CRITICAL
Remediation	Remove the backdoor from the system & make sure to close the port

Evidence

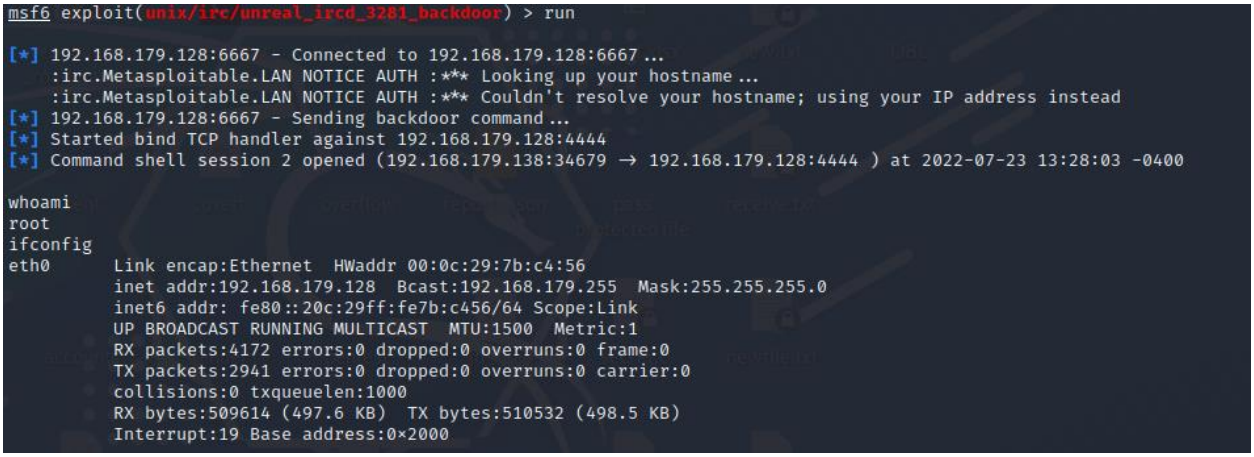
References

- Reference line 1
- Reference line 2

PENTEST BD

IPT-05: UnrealIRCd Backdoor Detection	
Location	192.168.179.128:6667
Description	A unrealircd backdoor has been detected in the target system. It allows remote code execution to the system
Impact	CRITICAL
Remediation	Remove the backdoor from the system and close the port if not needed.

Evidence



References

- Reference line 1
- Reference line 2

IPT-06: DistCC Daemon Command Execution	
Location	192.168.179.142:3632
Description	Vulnerable distccd service is running on the system. It allows attackers to exploit and execute arbitrary command on any system running distcc service.
Impact	CRITICAL

Remediation	Disable this service & close the port

Evidence

```
msf6 exploit(unix/misc/distcc_exec) > run

[*] Started bind TCP handler against 192.168.179.142:4444
[*] Command shell session 2 opened (192.168.179.138:34787 → 192.168.179.142:4444 ) at 2022-07-26 07:53:32 -0400

whoami
root
ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:0a:e5:0d
          inet addr:192.168.179.142  Bcast:192.168.179.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe0a:e50d/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:886614 errors:0 dropped:0 overruns:0 frame:0
          TX packets:803023 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:131745114 (125.6 MB)  TX bytes:239179937 (228.0 MB)
          Interrupt:16 Base address:0×2024
```

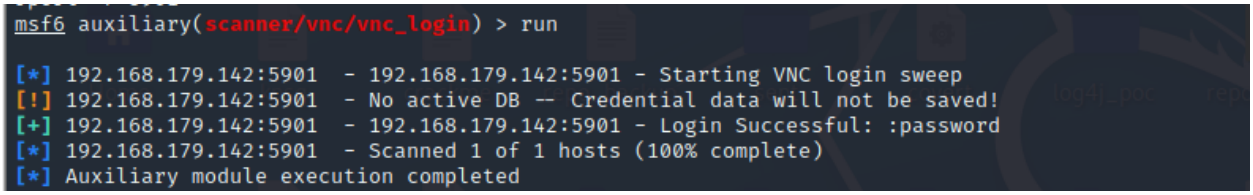
References

- Reference line 1
- Reference line 2

IPT-07: Weak Password In VNC	
Location	192.168.179.142:3632
Description	The VNC service is using weak password for authentication which is “password”
Impact	Medium
Remediation	Change the weak password. Apply a good password policy.

PENTEST BD

Evidence



References

- Reference line 1
- Reference line 2

Conclusion

There were several hosts in the network but only two is in scope at this time. We have considered it as a black box testing. So we weren't provided any information about the target. This was the first penetration test of CC Commerce. We have identified several critical issues that can be exploited. So we have provided the remediation plan. We have also added all the screenshots, vulnerability scanning report in the drive link. For additional information & documents, please check that drive.

PENTEST BD

THANKS