

**Vulnerability Assessment And Penetration Testing Of Empire Breakout Machine**

**Services provided to:**

***Empire Breakout Machine CTF***

**Version –V1.0**

V1 – February 12th, 2022

Prepared By: Abhishek Joshi

CyberBugs

Presented To: VulnHub

Empire Breakout



# CONFIDENTIALITY

In no event shall CyberBugs be liable to anyone for special, incidental, collateral or consequential damages arising out of the use of this information.

This document contains information, which is confidential and proprietary to CyberBugs and Empire Breakout. Extreme care should be exercised before distributing copies of this document, or the extracted contents of this document. CyberBugs is authorizing our point of contact at Empire Breakout. to view and disseminate this document as he/she sees fit in accordance with Empire Breakout data handling policy and procedures. This document should be marked “CONFIDENCIAL” and therefore we suggest that this document be disseminated on a “need to know” basis.

Address questions regarding the proper and legitimate use of this document to:

# DISCLAIMERS

CyberBugs Security

Abhishek joshi

The information presented in this document is provided as is and without warranty. Vulnerability assessments are a “point in time” analysis and as such it is possible that something in the environment could have changed since the tests reflected in this report were run. Also, it is possible that new vulnerabilities may have been discovered since the tests were run. For this reason, this report should be considered a guide, not a 100% representation of the risk threatening your systems, networks and applications.



1. **Contents**

[CONFIDENTIALITY 2](#_TOC_250018)

[DISCLAIMERS 2](#_TOC_250017)

1. [Purpose 4](#_TOC_250016)
2. [Scope 4](#_TOC_250015)
3. [Summary of Findings 5](#_TOC_250014)

[Open Port Vulnerabilty 6](#_TOC_250013)

[Source Code Information Disclosure 1](#_TOC_250012)0

[Admin Panel Disclosure 1](#_TOC_250011)2

[SMB Enumeration 1](#_TOC_250010)4

[Found Pass File 17](#_TOC_250009)

[Root Access 2](#_TOC_250008)0

1. [Conclusion 2](#_TOC_250000)2



1. **Purpose**

Empire Breakout has asked CyberBugs Security to perform a detailed security examination of their Machine. This Machinel was a vulnerable machine, and we were provided access to a system.

This testing effort took place in February and February of 2022, and concluded on February 12th 2014. Some preliminary findings were provided under separate cover, and this report is being presented to show the full results of our testing efforts and to make recommendations where appropriate.

1. **Scope**

The scope of this review was limited to a single Internet facing web application portal.This is an vulnerable CTF Machine. The Machine IP address under review was at the following addresses:

|  |  |
| --- | --- |
| **Target** | **IP Address** |
| Empire Breakout | 192.168.3.195 |

**Important Note:** This Machine Is Vulnerable CTF Machine of Vulnhub Which Is Empire Breakout Machine

This Machine Is Vulenrable Machine CyberBugs Cannot Do Any Illegal Activity This Report And Machine Was For Only Educational Perpouse and Training Perpouse

CyberBugs Is a Cyber Security Service Provider

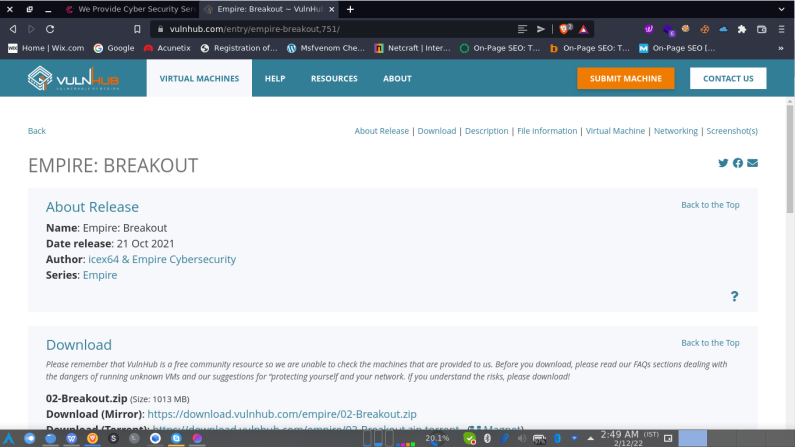
And Cyber Security Training Provider In Nagpur

Vist Our Wbsite:https://www.cyberbugs.in/

CyberBugs Provide All The Cyber Securiy Service:

1. Penetration Testing Services (VAPT)
2. Cyber Security Consulting
3. Create Security Polocies
4. Network Security And Monitoring
5. WAPT,MAPT,API Pentesting

**Figure 1 CTF Machine Empire Break Out**







1. **Summary of Findings**

In performing a detailed penetration study against Empire Breakout’s, CyberBugs security identified several issues of concern, but overall found the System to be built around a solid security model. Throughout this report we provide brief descriptions of each testing category and provide more detailed where our findings were negative.

The below table shows a breakdown of the vulnerabilities identified based on category and severity of risk. This table is followed by a detailed breakdown outlining each category. In the table below, a vulnerability listed under ‘Pending’ has been reported, where a vulnerability listed under ‘Fixed’, is a vulnerability that has been satisfactorily mitigated.

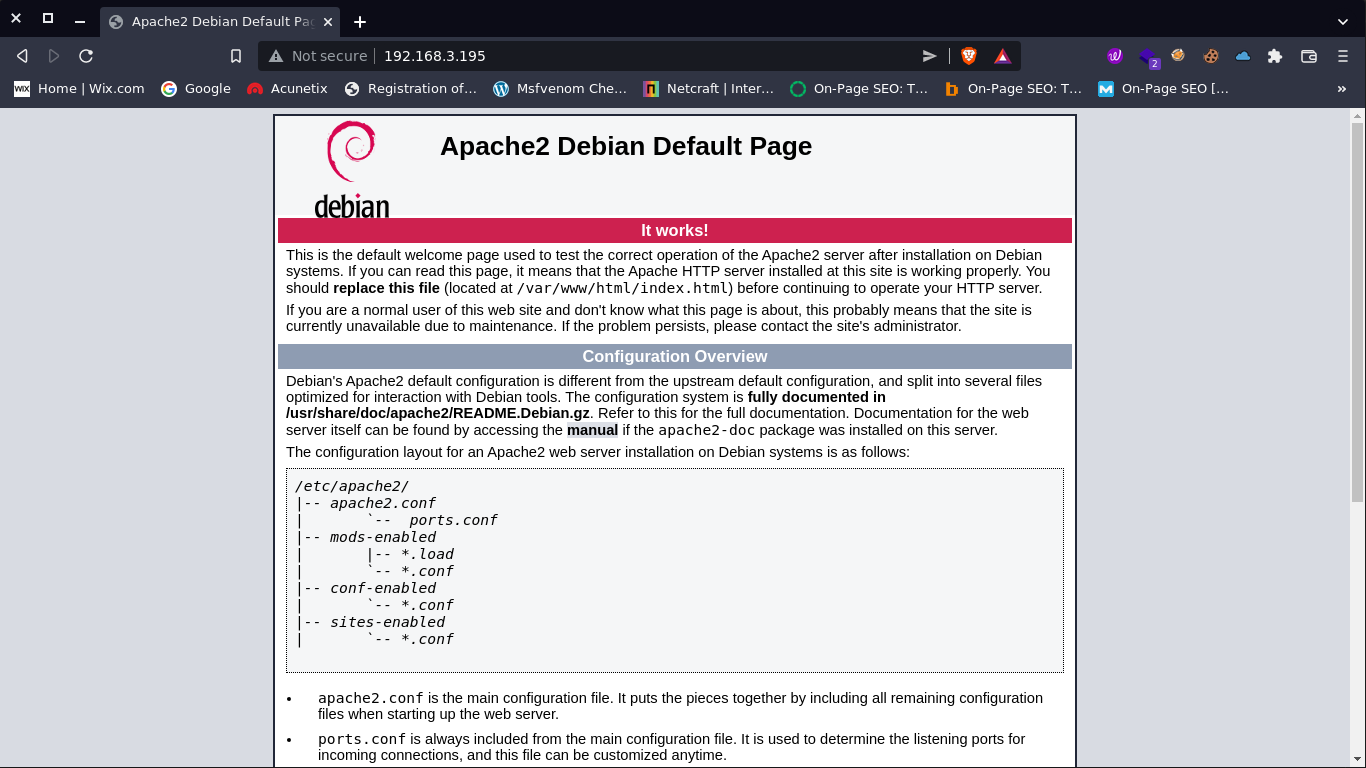
**Figure 2 -­‐ Findings Matrix**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Vulnerabilities tallied by Risk rating** | | | | | | |
| **Testing Category** | **High** | | **Medium** | | **Low** | |
| **Fixed** | **Pending** | **Fixed** | **Pending** | **Fixed** | **Pending** |
| Open Port Vulnerability |  | **1** |  |  |  |  |
| Source Code Information Disclosure |  | **1** |  |  |  |  |
| Admin Panel Disclosure |  |  |  |  |  | **1** |
| SMB Enumertaion |  |  |  |  |  | **1** |
| Found Pass File |  | **1** |  |  |  |  |
| Access Root User |  | **1** |  |  |  |  |



|  |  |
| --- | --- |
| Issue 1: Open Port Vulnerability | |
| **Risk:** | **HIGH** |
| Successful attack could result in Open Ports |
| **Complexity:** | **HIGH** |
| Attack requires all the ports and try to exploit vulnerability attacker knows about your network positure and perform attack |
| **Summary:**  Commonly Hacked Ports  Common vulnerable ports, such as SSH port 21 FTP port 22 are easily vulnerable to hackers. In your security tests, be sure to check these commonly hacked TCP and UDP ports:  TCP port 21 — FTP (File Transfer Protocol)  TCP port 22 — SSH (Secure Shell)  TCP port 23 — Telnet  TCP port 25 — SMTP (Simple Mail Transfer Protocol)  CP and UDP port 53 — DNS (Domain Name Path)  TCP port 110 — POP3 (Post Office Protocol version 3)  TCP and UDP port 135 — Windows RPC  TCP and UDP ports 137–139 — Windows NetBIOS over TCP/IP  TCP port 1433 and UDP port 1434 — Microsoft SQL Server  hacker can take a advantages and exploit to gain a access on your Path and servers  Empire Breakout Have SMB port and Admin Pannel access port number attacker can do smb user enumeration and find the pass to do login on specific port  We can demonstrate this by performing the following steps:   1. Find The Target IP and Scan All the Ports And Vesrion Itself   target 01   1. Find Target IP Address Throug Scan Netwrok     nmap 02   1. Scan Target Port   **nmap ports 03**  **Details:**  Now you can see https,smb minserv ports are open machine have website services | |





**Recommended Resolution:**

CyberBugs Security recommends that, Sensitive ports should be closed or filter by the firewall and service version should be updated



|  |  |
| --- | --- |
| Issue 2: Source Code Information Disclosure | |
| **Risk:** | **HIGH** |
| Successful attack could result source code info disclosure |
| **Complexity:** | **HIGH** |
| This attack requires the sensitive information on source code which may help attackers to find user and pass or any other vulnerable parametes |
| **Summary:**  Source code intended to be kept server-side can sometimes end up being disclosed to users. Such code may contain sensitive information such as database passwords and secret keys, which may help malicious users formulate attacks against the application.  We can demonstrate this by performing the following steps:   1. open a website 2. go to source code 3. at the end of the code i found a encryption key which is brainfuck decode 4. after decoding with brainfuck i found the password only   encryption in source code 05  decode success 06  Found a Key .2uqPEfj3D<P'a-3  **Recommended Resolution:**  Server-side source code is normally disclosed to clients as a result of typographical errors in scripts or because of misconfiguration, such as failing to grant executable permissions to a script or directory. Review the cause of the code disclosure and prevent it from happening. | |



|  |  |
| --- | --- |
| Issue 3:Admin Panel Disclosure | |
| **Risk:** | **LOW** |
| Attacker found the admin panel using port 20000/10000 |
| **Complexity:** | **LOW** |
| This attack only requires the admin panel and try to logged in admin panel |
| **Summary:**  Admin panel disclosure attacker can know about your website structure network and admin panel now attcaker can try loged in in unauthorized way.  We can demonstrate this by performing the following steps:   1. open a website and found admin panel on 20000 port or 10000 port 2. we alredy have password which i found on source code   1000,2000 port are open 07  login found 08  **Recommended Resolution:**  CyberBugs Security recommends that sensitive port was closed and admin panel is not communcable publically and also secure admin panel | |



|  |  |
| --- | --- |
| Issue 4:SMB Enumeration | |
| **Risk:** | **LOW** |
| Attacker found the local user directory |
| **Complexity:** | **LOW** |
| This attack requires the admin panel username |
| **Summary:**  SMB port was open and vulnerable so we easily enumertae the smb username using enum4linux  We can demonstrate this by performing the following steps:   1. SMB port is open 2. Enumerate username using enum4linux 3. we alredy have pass gather using source code 4. after we try login admin panel and successfully logged in     smb port open 09  enum4linux 10    dound lococal user 11  Found user /user/cyber  login success 12  login succes 13  **Recommended Resolution:**  CyberBugs Security recommends that sensitive port was closed and admin panel is not communcable publically and also secure admin panel | |



|  |  |
| --- | --- |
| Issue 5:Found Pass File | |
| **Risk:** | **HIGH** |
| Attacker found the pass file on /var/backups/.old\_pass.bak |
| **Complexity:** | **HIGH** |
| This attack requires the root user password |
| **Summary:**  Attacker can find the user and password when they take a access.Attacker try to gain a access of root user to do any illegal activity  We can demonstrate this by performing the following steps:  1. after successfully login we go to shell terminal  2. go to /home/cyber we found two file user.txt and tar file  3. user.txt file have FLAG we found a flag now  4. after we see on tar we go to /var/backup we found the pass file   1. then we convert .bak file to tar then using a tar command we successfully found the pass of root uset     found flag 14    we found a flag 3mp!r3{You\_Manage\_To\_Break\_To\_My\_Secure\_Access}      found old pass but access denied 15  found .old\_pass.bak  tar file is there 16    tar file is there using tar file lets convert .bak to .tar and retrive the root user pass  found the pass from old pass 17  Found pass Ts&4&YurgtRX(=~h  **Recommended Resolution:**  CyberBugs Security recommends no sensitive file will be disclosue and all the file should be fully encrypted and secure no one can access the file easily. | |



|  |  |
| --- | --- |
| Issue 6:Root Access | |
| **Risk:** | **HIGH** |
| Attacker can access the root using reverse shell |
| **Complexity:** | **HIGH** |
| This attack requires the root user |
| **Summary:**  Attacker can perfom reverse shell and access the root user  We can demonstrate this by performing the following steps:   1. after successfully gather all the things 2. we use reverse shell and gain the acess of the root user   shell form github  do reverse shell 18    root access success 19      you can see here we gather the access of root easily      **Recommended Resolution:**CyberBugs Security recommends fix all the previous vulnerability to secure your enviroment so no one can access your system | |

1. **Conclusion**

Overall, we found that machine is vulnerable attacker easily gather the username and password of login panel as well as the root user password.CyberBugs checks all the possibilities to gain the access of system.

The following list is a summary of items requiring remediation:

|  |  |  |  |
| --- | --- | --- | --- |
| **Description** | | **Risk Rating** | **Page Ref** |
| **Issue 1** | Open Port Vulnerability | High | 6 |
| **Issue 2** | Source Code Information Disclosure | High | 10 |
| **Issue 3** | Admin Panel Disclosure | Low | 12 |
| **Issue 4** | SMB Enumertaion | Low | 14 |
| **Issue 5** | Found Pass File | High | 17 |
| **Issue 6** | Root Access | High | 20 |