

**Vulnerability Assessment And Penetration Testing Of empire lupinone Machine**

**Services provided to:**

***empire lupinone Machine CTF***

**Version –V1.0**

V1 – February 15th, 2022

Prepared By: Abhishek Joshi

CyberBugs

Presented To: VulnHub

Empire lupinone



# 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 lupinone. 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 lupinone. to view and disseminate this document as he/she sees fit in accordance with empire lupinone 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)

[Found SSH Private KEY 1](#_TOC_250012)0

[Access System 1](#_TOC_250011)6

1. [Conclusion](#_TOC_250000) 22



1. **Purpose**

empire lupinone 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 15th 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 lupinone | 192.168.3.20 |

**Important Note:** This Machine Is Vulnerable CTF Machine of Vulnhub Which Is empire lupinone 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

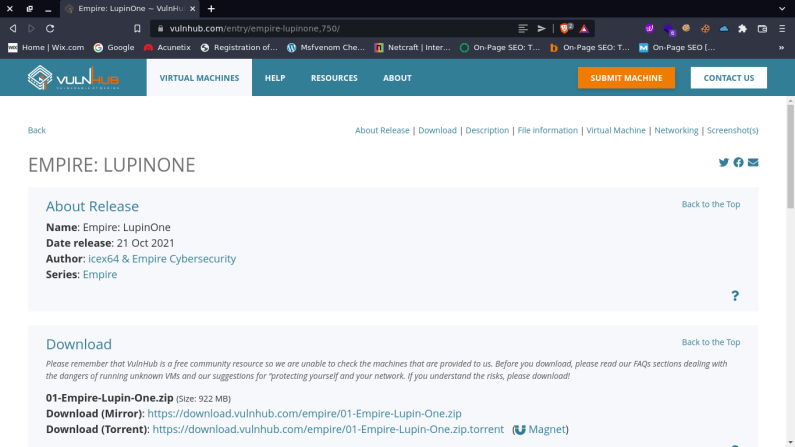
And Cyber Security Training Provider In Nagpur

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 Lupinone**







1. **Summary of Findings**

In performing a detailed penetration study against empire lupinone’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** |  |  |  |  |
| Found ssh private key |  | **1** |  |  |  |  |
| Access System |  | **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 lupinone Have ssh port so attacker find how to exploit and access machine using ssh port  We can demonstrate this by performing the following steps:   1. Find The Target IP and Scan All the Ports And Vesrion Itself   01 target   1. Find Target IP Address Throug Scan Netwrok        1. Scan Target Port   **02 nmap**  **Details:**  Now you can see https,ssh port was open | |



****

**Recommended Resolution:**

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



|  |  |
| --- | --- |
| Issue 2: Found SSH Private Key | |
| **Risk:** | **HIGH** |
| Successful attack could result found ssh private key |
| **Complexity:** | **HIGH** |
| This attack requires the sensitive information |
| **Summary:**  Hidden file is accessible on empire lupinone machine on robots.txt ~myfiles cant be access but found ~ this location using this gather the ~secret/ filr and then inton this file we get a hidden file using fuzzing ~secret/.mysecret.txt  We can demonstrate this by performing the following steps:   1. open a website 2. go to ~myfiles not accessible 3. using fuzzing found ~secret file 4. after find ~secret file we found hidden file .mysecret.txt file on this file have hashcode 5. then decode using base58 found ssh private key   04 robots.txt  05 myfiles  06 gobuster  07 wfuzz find secret file  08 secret directory  09 fuff tool  10 found mysecret txt file  11 found hash on my secret  12 found ssh private key  **Recommended Resolution:**  sensitive directory was not accessible and also dont save any sensitive file and ssh key should be fully encrypted with symmetric or asymmetric algorith use always strong hash algorithm | |



|  |  |
| --- | --- |
| Issue 3:Access System | |
| **Risk:** | **HIGH** |
| Attacker found the pass of ssh |
| **Complexity:** | **HIGH** |
| This attack requires the root access |
| **Summary:**  Attacker can find the user and password and gain the access of ssh  We can demonstrate this by performing the following steps:  1. after successfully gain the ssh private key hash  2. crack the hash using john  3. found password and gain the access of system  12 found ssh private key  13 save ssh private key id_rs  14 generate id_rsa hash using johnssh2  15 hash file  16 crack hash using john found pass ssh  16 gain ssh successfully  17 found flag  we found a flag 3mp!r3{I\_see\_That\_You\_Manage\_To\_Get\_My\_Bunny}          **Recommended Resolution:**  CyberBugs Security recommends no sensitive file will be disclosue and all the file should be fully encrypted and secure also password shoul be strong atlest 12-24 character long | |

1. **Conclusion**

Overall, we found that machine is vulnerable attacker easily gather the username and password of sshl and gain the access of system .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** | Found SSH Private Key | High | 10 |
| **Issue 3** | Access SSH Port | High | 16 |