Professor: Paul Dunn

Name: Muhammad Zainul Zahid

Date: 12/1/2023

MySQL exploit using FTP

SUBMIT (5pts) what is the IP of your Kali linux machine?

-192.168.85.130

(5pts) what is the IP of your target machine?

-192.168.85.132

(5pts) What command did you use to find the IP of the target?

nmap -sP 192.168.85.0/24

(5pts) What command did you run to show that MySQL is running?

Nmap -script=mysql-info 192.168.85.132

(5pts) Take a screenshot showing your connection to Metasploit right after you run the python command (this one should show ‘root@metasploitable’)

A screenshot of a computer program

Description automatically generated

(5pts) Take a screenshot of MySQL after you connect with your globalID from the Kali terminal.

A screenshot of a computer

Description automatically generated

A screenshot of a computer program

Description automatically generated

(5pts) Take a screenshot of MySQL showing the credit card info from the owasp10 database;

A screen shot of a computer

Description automatically generated

A screen shot of a computer

Description automatically generated

(5pts) Show the credit card information from the OWASP database.

A screen shot of a computer

Description automatically generated

Synopsis

In order to comprehend cybersecurity vulnerabilities, this report details the hands-on investigation of hashcode cracking using Kali Linux, Metasploitable, and CVE search. The analysis considers the learning objectives, makes conclusions, and provides particular suggestions for improving security protocols to fend off such attacks.

Using Kali Linux, Metasploitable, and CVE search, the goal of this exercise was to obtain practical insight into the techniques and tools used in hashcode cracking. Several methods were used through practical experience to crack hashcodes, highlighting the importance of comprehending and strengthening security protocols to reduce vulnerabilities.

What Was Learned:

The extensive toolkit available for penetration testing and security assessments was made evident through the use of Kali Linux. This toolkit, which included Nmap, John the Ripper, and Wireshark, among other tools, offered a useful environment for examining system vulnerabilities. In particular, dictionary attacks were made possible by tools like John the Ripper, demonstrating how easily weak passwords can be cracked.

As a system designed to be intentionally vulnerable, Metasploitable played a crucial role in modeling real-world exploitation scenarios. Vulnerabilities like default credentials, unpatched services, and incorrectly configured settings were exploited through Metasploit framework exercises, highlighting the vital need of routine patching and system updates.

Investigating CVE search databases led to a better comprehension of known vulnerabilities and the exploits linked to them. As a result, vulnerability assessment could be done with greater knowledge, highlighting the necessity of taking preventative action against known threats.

Concluding remarks:

Hashcode Vulnerabilities: The exercise highlighted the serious flaws in systems and highlighted how simple it is to crack hashcodes using easily accessible tools and methods.

Patching is important because a lot of the vulnerabilities that were exploited during the exercise were known vulnerabilities, or CVEs. This means that timely system updates and patches are essential to preventing exploitation.

Stronger Authentication is Required: The need for strong authentication techniques was highlighted by weak password hashing algorithms and easily cracked passwords.

Recommendations:

It is essential to improve password policies. Promoting the use of long, complicated passwords in addition to multi-factor authentication can significantly reduce the likelihood of hashcode cracking. Security is further strengthened by teaching users about password hygiene and using password managers to enforce strong, one-of-a-kind passwords.

Routine security audits are essential. System flaws can be proactively found by performing regular penetration tests and vulnerability assessments. This enables companies to address vulnerabilities prior to their malicious exploitation.

It's critical to keep up with security patches and CVEs. By ensuring that important updates are applied promptly, a strong patch management system can minimize the window of opportunity for potential attacks.

Last but not least, an organization's cybersecurity posture can be greatly strengthened by promoting a security-conscious culture through ongoing user education. Preventing breaches can be greatly aided by educating staff members about best practices, spotting phishing attempts, and encouraging a proactive attitude toward cybersecurity awareness.

Preventive Actions:

Using robust hashing algorithms, such as Argon2 or bcrypt, is essential for safely storing passwords and making them much more difficult to crack. Moreover, security can be improved by prohibiting the reuse of passwords and requiring frequent password changes.

By dividing vital systems into separate segments, network segmentation reduces the effect of security lapses and keeps possible threats contained. In the event of a breach or ransomware attack, regular data backups—ideally kept in safe, offline locations—act as an efficient mitigation strategy against data loss.

Securing sensitive data during transmission and at rest can be achieved by implementing strong encryption standards, which also guard against unwanted access and possible data breaches.

In summary:

To sum up, the investigation into hashcode cracking with Metasploitable, Kali Linux, and CVE search has highlighted the critical flaws that are present in many systems. The suggestions made highlight the necessity of strong authentication procedures, proactive cybersecurity measures, and ongoing vigilance to protect against changing threats. This encounter highlights the necessity for a multi-layered, proactive approach to cybersecurity to protect against emerging vulnerabilities in an ever-evolving digital landscape.