**ASSIGNMENT**

|  |  |  |  |
| --- | --- | --- | --- |
| **COURSE** | Deep Packet Inspection | **ASSIGNMENT NO** | Final 2 |
| **MODULE** | DPI | **ASSIGNMENT DATE** | 14/09/2024 |
| **STUDENT NAME** | Konganti Chaithanya kumar | **SUBMISSION DATE** | 14/09/2024 |

**Analyze the pcapng file and send the detailed report.**

The **machine.pcapng** file analysis reveals several key details :

**1. FTP Brute-Force Login Attempts:**

The network capture shows numerous login attempts to an FTP server using the username **"msfadmin".** Different passwords are systematically tried, indicating a brute-force attack.

The FTP server responds with various status codes:

* **331:** Indicates that a password is required for the provided username.
* **530:** Indicates an incorrect username or password.
* **230:** Indicates a successful login.

After multiple failed attempts, the attacker successfully logs in using the password **"msfadmin,"** as shown by:

* **USER:** msfadmin
* **PASS:** msfadmin
* **331** Please specify the password.

**230 Login successful.**

Following the successful login, the attacker attempts.

The attacker uses the FTP to transfer data to the server:

150 Ok to send data.

The file transfer is completed successfully.

**2. Captured Credentials:**

Within the network traffic, plaintext credentials were observed:

**Email:** vinaykumarg007@hotmail.com

**Password:** pass123@me

* 226 Transfer complete.
* 221 Goodbye.
* 331 Please specify the password.
* PORT 10,10,10,40,132,177
* 200 PORT command successful. Consider using PASV.

**3. Web Application Attack:**

The network traffic captures an HTTP GET request to a vulnerable web application running on **10.10.10.60:**

**GET /dvwa/vulnerabilities/sqli/?id=1&Submit=Submit HTTP/1.1**

**Host:** 10.10.10.60

**URL** path /dvwa/vulnerabilities/sqli/ indicates an attempt .

* This type of attack can be used to extract data from the database, modify it, or perform administrative operations, depending on the privileges of the web application.

**4. Server Responses:**

The server responds with HTTP status codes:

**200 OK:** Indicates successful processing of the requests, suggesting the attacker might be able to retrieve data via the SQL injection.

**400 Bad Request:** Indicates that some of the HTTP requests were malformed, possibly as part of probing or attempting different injection methods.

**5. General Observations:**

* The plaintext credentials and sensitive data in the network traffic indicates a lack of encryption (e.g.,using FTP ,FTPS, SFTP).
* Brute-force login attempts suggest weak or default passwords were in use, emphasizing the need for strong password policies.
* The SQL injection attempts highlight the importance of secure coding practices and proper input validation in web applications.

**Recommendations:**

* Use secure protocols like FTPS, SFTP, or HTTPS to prevent interception of plaintext data.
* Apply MFA and strong password policies to prevent brute-force attacks.
* Use an IDS to identify unusual login patterns or potential brute-force attempts.
* Implement security measures such as input validation, prepared statements.
* unauthorized data transfers.
* This analysis provides a detailed overview of the suspicious activities captured in the pcapng file.

The login attempts you provided seem to be part of an FTP login process where multiple passwords were tried before eventually succeeding with the password "msfadmin".

* **Multiple Failed Attempts:** The majority of the attempts result in **530 Login incorrect**, indicating the password provided was not correct.
* **Successful Login:** The attempt using USER msfadmin and PASS msfadmin resulted in a 230 Login successful, which means the username and password combination was finally correct.
* **FTP Server Details:** The server identified is running of the Very Secure FTP.
* **Error Message:** The HTTP/1.1 400 Bad Request response at the end suggests a possible attempt to interact with an HTTP server after the FTP login.

FTP login issues, use the correct username and password.

**Login attempts:**

**----------------------------------------------------------------------------------**

* USER msfadmin
* 331 Please specify the password.
* **PASS 123456**
* 530 Login incorrect.

----------------------------------------------------------------------------------

* USER msfadmin
* 331 Please specify the password.
* **PASS 12345**
* 530 Login incorrect.

-----------------------------------------------------------------------------------------

* USER msfadmin
* 5331 Please specify the password.
* **PASS password**
* 530 Login incorrect.

---------------------------------------------------------------------------------------------

* USER msfadmin
* 331 Please specify the password.
* **PASS password1**
* 530 Login incorrect.

--------------------------------------------------------------------------------------------------

* USER msfadmin
* 331 Please specify the password.
* **PASS 123456789**
* 530 Login incorrect.

----------------------------------------------------------------------------------------------

* USER msfadmin
* 331 Please specify the password.
* **PASS 12345678**
* 530 Login incorrect.

----------------------------------------------------------------------------------------------

* USER msfadmin
* 331 Please specify the password.
* **PASS 1234567890**
* 530 Login incorrect.

----------------------------------------------------------------------------------------------

* USER msfadmin
* 331 Please specify the password.
* **PASS abc123**
* 530 Login incorrect.

------------------------------------------------------------------------------------------

* USER msfadmin
* 331 Please specify the password.
* **PASS computer**
* 530 Login incorrect.
* USER msfadmin
* 331 Please specify the password.
* **PASS tigger**
* 530 Login incorrect.

----------------------------------------------------------------------------------------------

* USER msfadmin
* 331 Please specify the password.
* 530 Login incorrect.
* USER msfadmin
* 331 Please specify the password.
* **PASS qwerty**
* 530 Login incorrect.

----------------------------------------------------------------------------------------------

* USER msfadmin
* 331 Please specify the password.
* **PASS money**
* 530 Login incorrect.
* USER msfadmin
* 331 Please specify the password.
* **PASS carmen**
* 530 Login incorrect.
* USER msfadmin
* 331 Please specify the password.
* **PASS mickey**
* 530 Login incorrect.

----------------------------------------------------------------------------------------------

* USER msfadmin
* 331 Please specify the password.
* **PASS secret**
* 4530 Login incorrect.

----------------------------------------------------------------------------------------------

* USER msfadmin
* 8331 Please specify the password.
* **PASS summer**
* 530 Login incorrect.

----------------------------------------------------------------------------------------------

* USER msfadmin
* @331 Please specify the password.
* **PASS internet**
* 530 Login incorrect.

--------------------------------------------------------------------------------------------------

* USER msfadmin
* G331 Please specify the password.
* **NO PASS a1b2c3**
* 530 Login incorrect.
* USER msfadmin
* 331 Please specify the password.
* 530 Login incorrect.

----------------------------------------------------------------------------------------------

* USER msfadmin
* 331 Please specify the password.
* **PASS service**
* 530 Login incorrect.
* USER msfadmin
* 31 Please specify the password.
* 530 Login incorrect.

**Completed Successful Login**

**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***

* USER msfadmin
* 331 Please specify the password.
* **PASS msfadmin**
* **230 Login successful.**

**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***