Date 10/06/2022

Information security audit:

This audit is conducted by bentalem abate

Basic audit information

1. This audit was conducted on an environment due to be released to production in few next days
2. This audit contains some findings,risks,exposures and recommendation that i have found during my testing
3. This report is relevant for the period of audit - Jone 2022
4. This survey made by me and contains only mine testing perspective

Bentalem abate

Best regards

Table of content

Chapter 1 - Audit Summary

Summary

This audits was conducted to assess the security level of the company to reduce the risks to the system's integrity.

The test was conducted in a format that would enable the company to identify and deal with the main risks in a manner that would eliminate the chances of realizing the damage to the system.

Method

The survey was conducted in a format that would enable the company to identify and deal with the main risks in a manner that would reduce or eliminate the chances to realize exposure to damage to the company's system.

This audit was developed in known testing methodologies to accomplish best execution but it's necessary to note that it is not possible to cover all possibilities of exploiting the system.

Test Objectives

★ Performing an examination that simulates a potential attacker who tries to attack the system. In accordance with the results, to assess the range of risks in a manner that will enable fix them as quickly as possible

★ Receive a current and objective assessment of the system security level that would enable the IT system department to develop and update different all their tools and give some professional feedback of their current security system level in order to keep their professionality.

General Impression

During the audit, it was found that the general level of security of the system is low and needed fast remandition.

Chapter 2 - Methodology

The stage of the audit

The audit includes 4 stage

Analysis the result

The audit result was analyzed in the following configuration

- The subject that was tested:in this exclusive audit,it was tested the company's technology system level before published to production
- The description of the problem:it was given the extended description of the finding during this test:for example, that allows an attacker to get remote code execution on the company's system.
- Finding the examination:in the purpose of this section it was documented all the existing situation of the system and all security vulnerabilities findings during the audit and the findings are often accompanied by screenshots

- Severity level:the severity level is determined as follows:the assessed level of risk resulting from the combination of scenarios of threats.
- Determination of the exploitability:the probability in which a vulnerability could be exploited in the system is determined by the following factors:
    - capabilities of the source of the threat
    - Effectiveness of controls to minimize threat

Determination of the probability of the threat

Exploitability	Description
High	The source of the threat is highly capable and the controls that can prevent the exploitation of the weakness is ineffective
Medium	The source of the threat is highly capable but the controls may prevent the exploitation of the weaknees somehow
Low	The source of threat is not capable or there are some controles preventing the exploitation of the weakness

<u>Determining the level of the damage</u>: Estimating the damage that can be caused by successful exploitation of a defect by a threatening scenario.

Damage	Description

High	Executing the threat may lead to several damage:
	  Financial damage,legal or regulatory damage by lawsuits and fines,Damage to company's image that can lead to severe loss of clients,
	  Full loss of management control

Medium	Executing the threat may lead to several damage:
	  Substantial financial damage,substantial legal/regulatory damage by lawsuits and fines,substantial damage to company's image that can lead to severe loss of clients,
	  Partial loss of management control

Low	Executing the threat may lead to several damage:
	  Certain financial damage,certain legal/regulatory damage by lawsuit and fines,
	  Certain damage to company's image, certain loss of management control

Determining the level of the risk:The level of risk is determined by multiplying the level of probability of realizing the threat and the magnitude of the damage Its realization.

Chapter 3 - finding summary

The following list is all finding,vulnerabilities and examined subjects that was found and given during the audit

#	Examine subjects	Description	Overall risk
1	Exposing default web page	It was found that the application is expose default wep application	Low
2	Exposing default server errors	It was found that the application is expose default server error which can lead to exposing critical data	Low
3	Exposing users credentials	During the audit it was found that application is exposing user's credentials	High
4	Exposing critical data in web page	During the scanning stage it was found that application is exposing critical data like smb sharing directory in web page	High
5	Broken access control	It was found that the application allowing regular user increasing his privileges	High

Findings and Explosures

1. Exposing default web page

Finding summary

During the audit it was found that the application exposes default windows web application web page with Microsoft-IIS/10.0 version.

Exploitable:Low

Severity:Low

Overall:Low

Risk Details:

In this case the application exposes default windows web application web page with its version.exposing application version may lead to help an adversary to collect overall technology system information which help him during his attack performing stage.

Recommendations

As part of taking complete security measures it is highly recommended not exposing files or pages not necessarily.

It's highly recommended to take down exposing of default web applications.

The following screenshots describe the exposing of the information
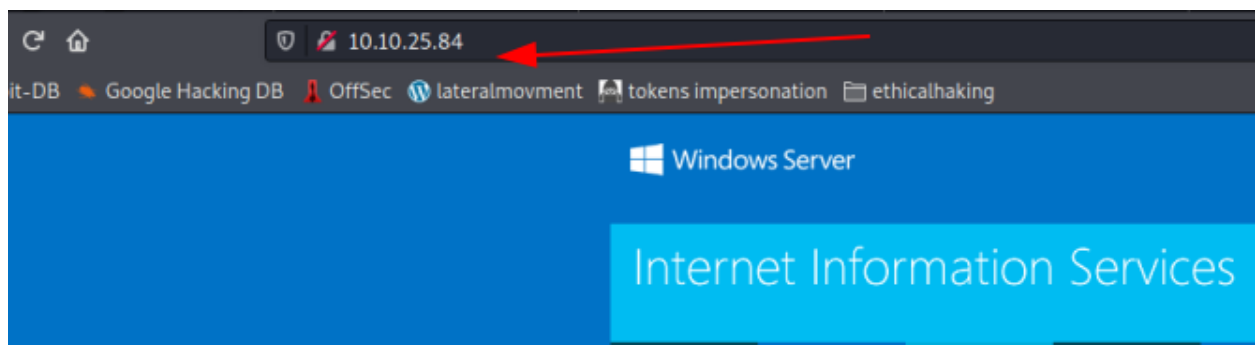
2.Exposing default server errors

Finding summary:

It was found that the application is exposing default server error.It definitely provides some interesting information to possible adversaries about your system (operating system, web server type and version).
Exploitable:Low

Severity:Low

Overall:Low

Risk Details:

During directory scanning part it was found that the application is exposing default

web application server errors as part of respond of broken request

Recommendations

As part of secured coding, it is highly recommended creating one fixed

component "page not found" and returning it as responding of broke request

The following screenshots describe the exposing of the information

Server Error in '/' Application.

Runtime Error

Description: An application error occurred on the server. The current custom error settings for this application prevent the details of the application error from being viewed remotely (for security reasons). It co

Details: To enable the details of this specific error message to be viewable on remote machines, please create a <customErrors> tag within a "web.config" configuration file located in the root directory of the cui

```
<!-- Web.Config Configuration File -->

<configuration>
    <system.web>
        <customErrors mode="Off"/>
    </system.web>
</configuration>
```

3.Exposing users credentials

Finding summary:

During the audit it was found that the application is exposing the user's credentials.as part of enumeration of smb it was found that in one smb sharing folder there was one user's credential file.these credentials may lead to completely control the application server remotely utilizing open RDP protocol.

Exploitable:Medium

Severity:High

Overall:High

Risk Details:

During smb enumeration it was found that the application allows smb connection with broken credentials.in one smb sharing directory found user's credentials which may lead to full foothold on server by using an open RDP protocol.
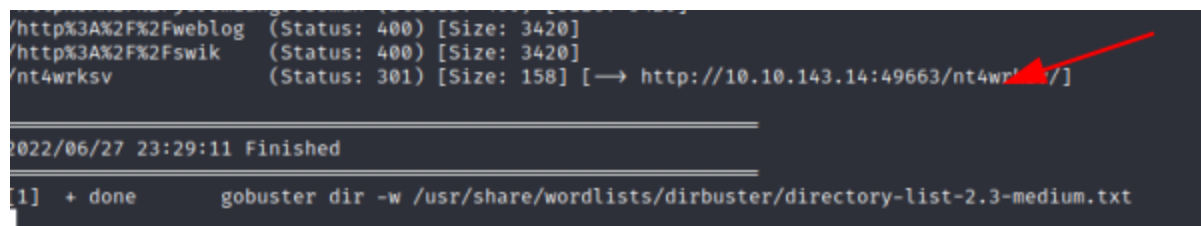
Recommendations

It was discovered that the application's prevent controls are disabling RDP connecting utilizing founded credentials,addnitaily

It is recommended that the application has to prevent the smb connection with broken credentials

It is highly recommended that the application has preventing putting down critical file in smb sharing

The following screenshots describe the exposing of the information


```
/http%3A%2F%2Fweblog   (Status: 400) [Size: 3420]
/http%3A%2F%2Fswik     (Status: 400) [Size: 3420]
/nt4wrksv              (Status: 301) [Size: 158] [→ http://10.10.143.14:49663/nt4wr    /]

2022/06/27 23:29:11 Finished

[1]  + done      gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
```

[User Passwords - Encoded]
Qm9iIC0gIVBBJCRXMHJEITEyMw==
QmlsbCAtIEp1dzRubmFNNG40MjA2OTY5NjkhJCQk

4.Exposing critical data in web page

Finding summary:

During the scanning stage it was found that application is exposing critical data like smb sharing directory in web page

Exploitable:High

Severity:High

Overall:High

Risk Details:

During the audit the application is exposing the smb sharing directory in the web page.this dangered option is allowing an adversary person to upload Malicious code file in smb client sharing and getting it in web pages.this functionality allows an adversary executing remote code execution attack.
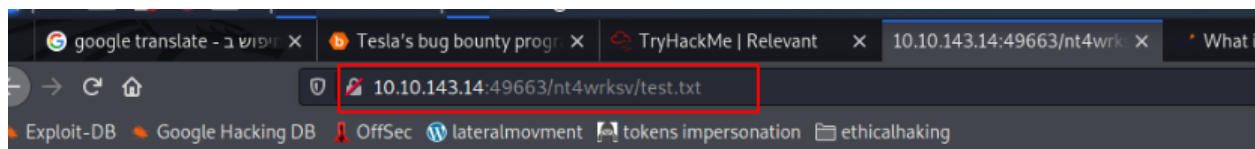
Recommendations

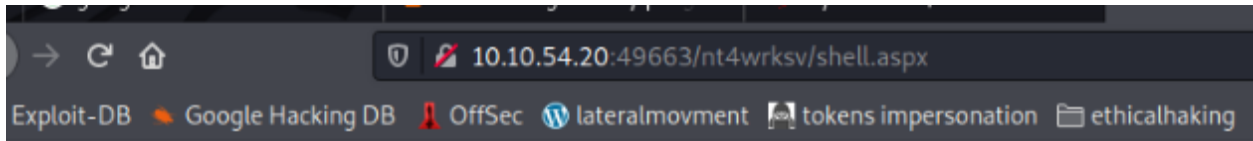It's highly recommended secured web application coding:

Preventing file disclosure in web page by coding correctly

In case the web application has to disclosure certain file it is highly recommended using suitable controls with clearly configuration that prevent uploading or attaching Malicious code files - control like web application firewall

The following screenshots describe the exposing of the information

5.Broken access control

Finding summary:

It was found that the application allowing regular user increasing his privileges

Exploitable:High

Severity::High

Overall::High

Risk Details:

By allowing seimpersonateprivilege right to regular user ,the application increased the probability to an adversary obtaining full control on the server.this specific user rights given to system administrators to allow them processing system process and threads and in this case this dangered rights given to regular user.

Recommendations

It's highly recommended to assess clearly and carefully conducting access control strategy

The following screenshots describe the exposing of the information

```
c:\Users\Bob\Desktop>whoami -priv
whoami -priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                  Description                              State

SeAssignPrimaryTokenPrivilege   Replace a process level token            Disabled
SeIncreaseQuotaPrivilege        Adjust memory quotas for a process       Disabled
SeAuditPrivilege                Generate security audits                 Disabled
SeChangeNotifyPrivilege         Bypass traverse checking                 Enabled
SeImpersonatePrivilege          Impersonate a client after authentication Enabled
```



```
c:\inetpub\wwwroot\nt4wrksv>PrintSpoofer.exe -i -c cmd
PrintSpoofer.exe -i -c cmd
[+] Found privilege: SeImpersonatePrivilege
[+] Named pipe listening ...
[+] CreateProcessAsUser() OK
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```