**-7) Perform port exploitation and describe possible remediations**

**port exploitation**

**misconfiguration**

**web application**

**Target machine – Metasploit and testfire.net, another domain**

**Commands used –**

**Nmap, dnsmap, lbd, dnsrecon, wafw00f, dnsenum,Dmitry,theHarvester.**

**Description –**

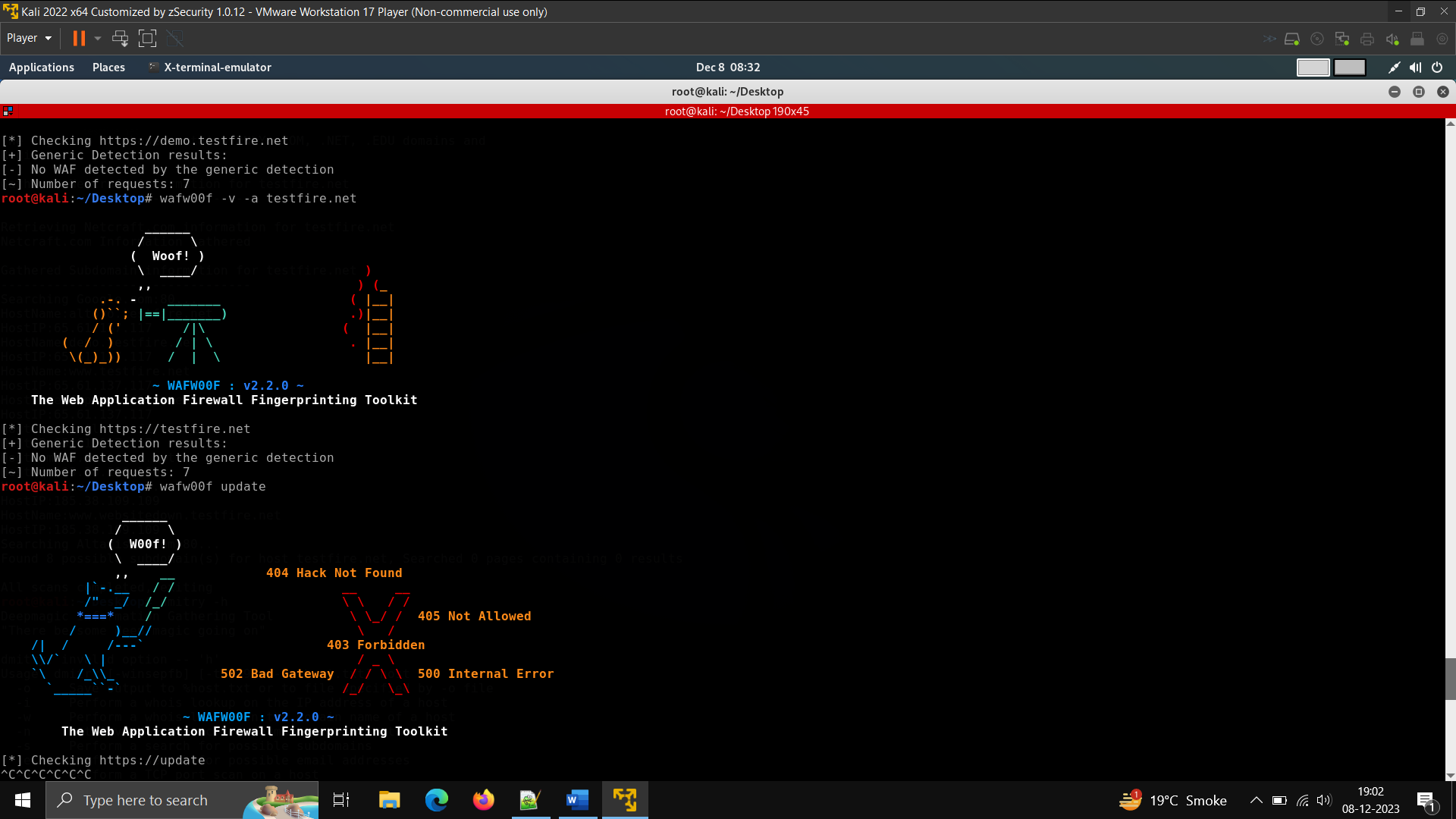
**Nmap is used scan all available Ips and open ports**

**Use -Pn when ping is disable**

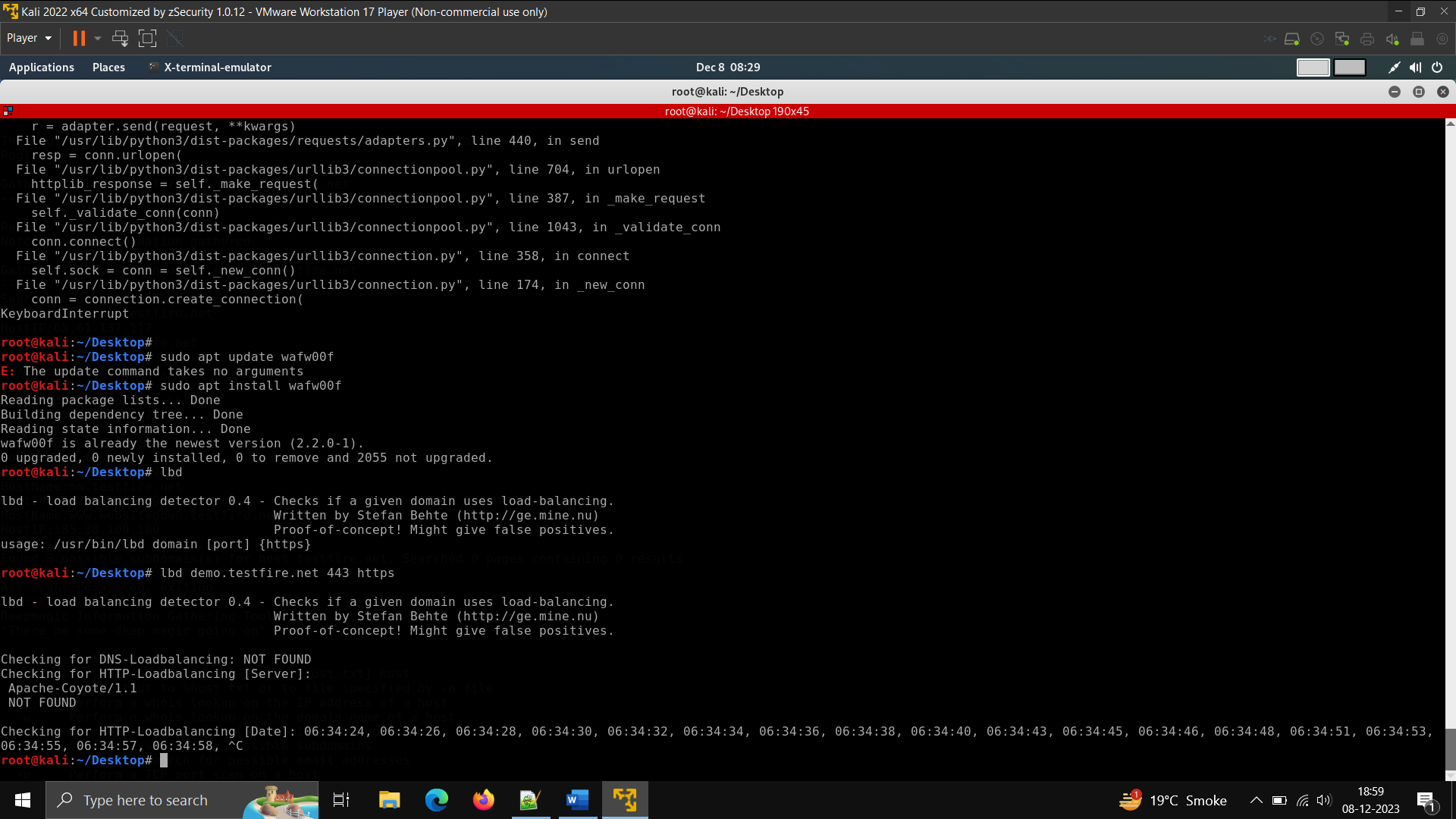
**Use -sV used for version**

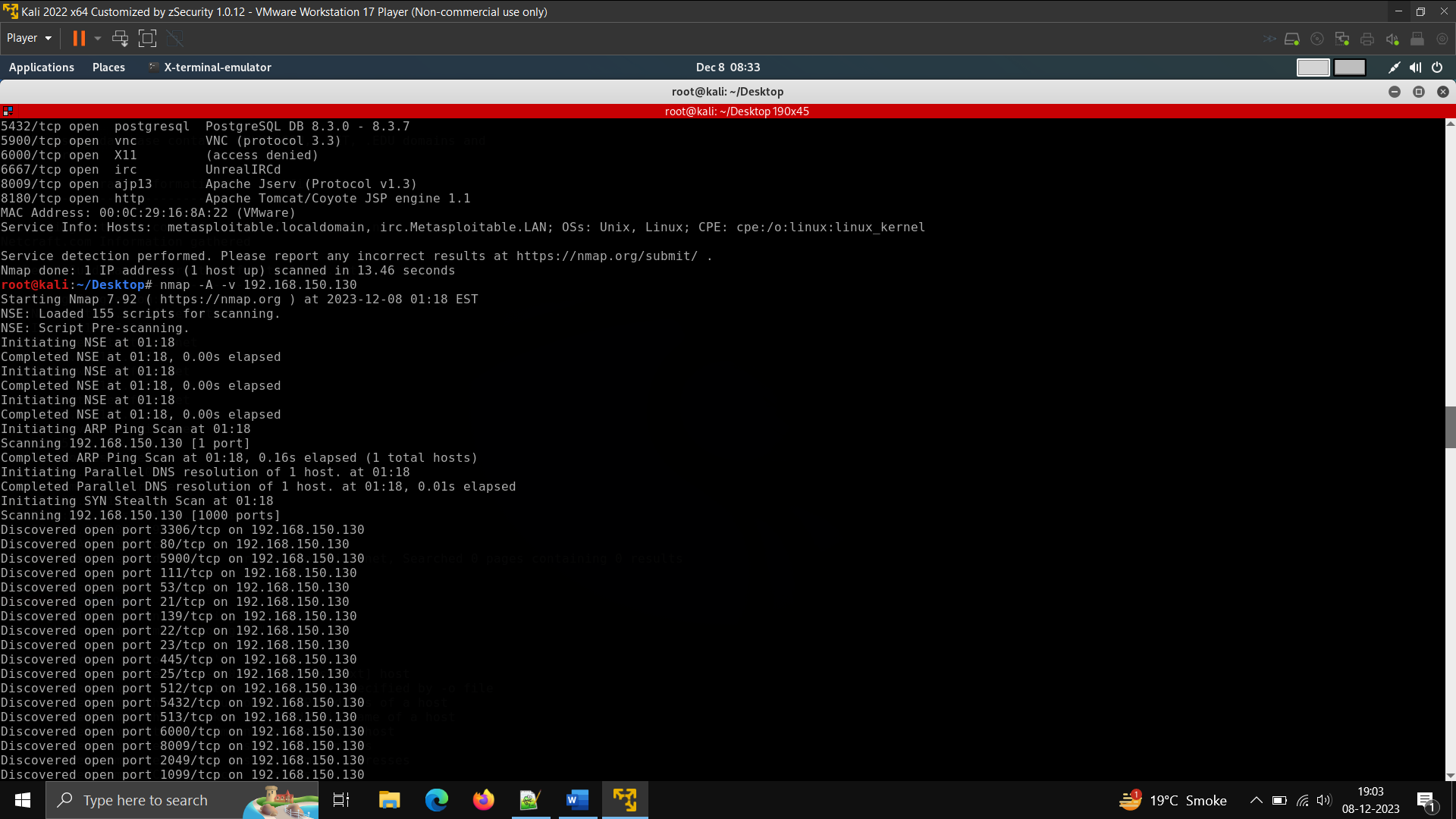
**……………………….**

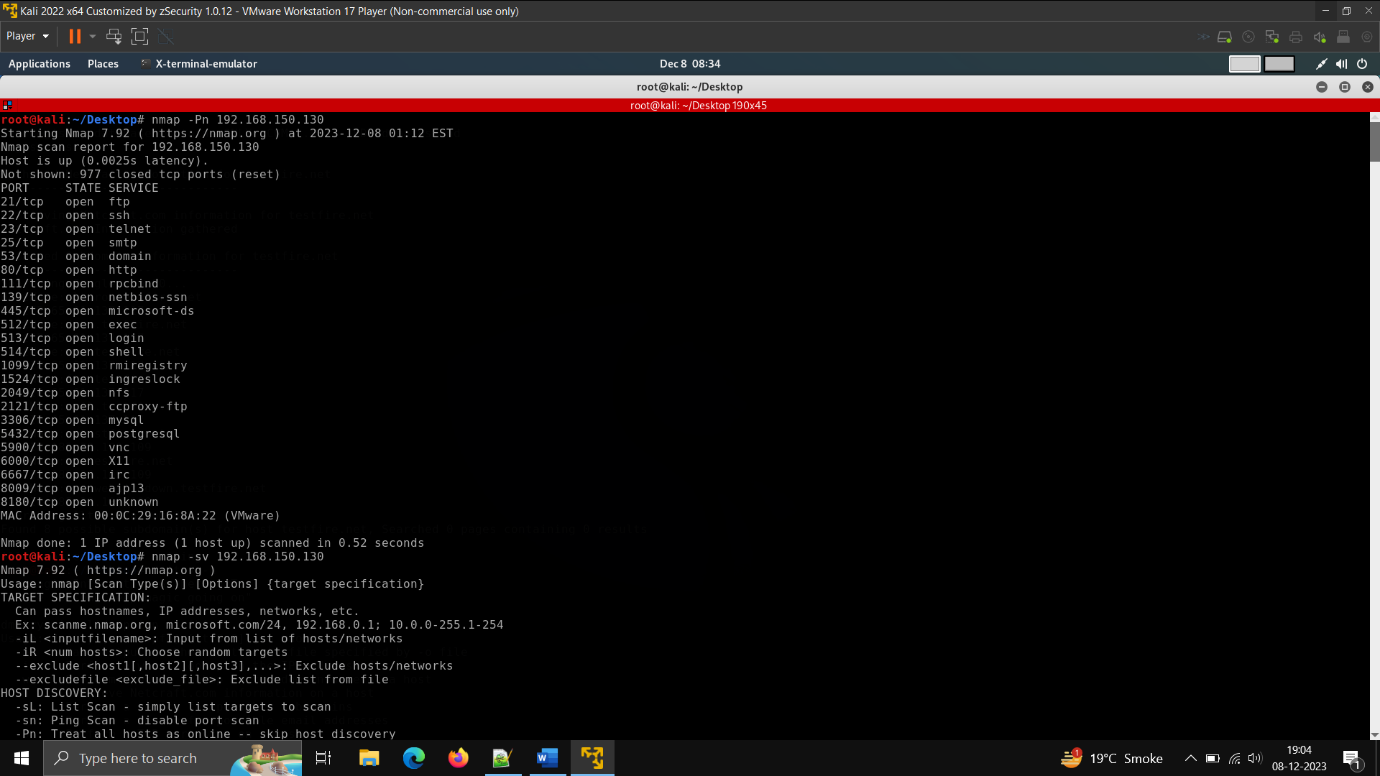
**Wafw00f – used for detecting firewall.**



**Lbd – for testing that the server has load balancer or not.**

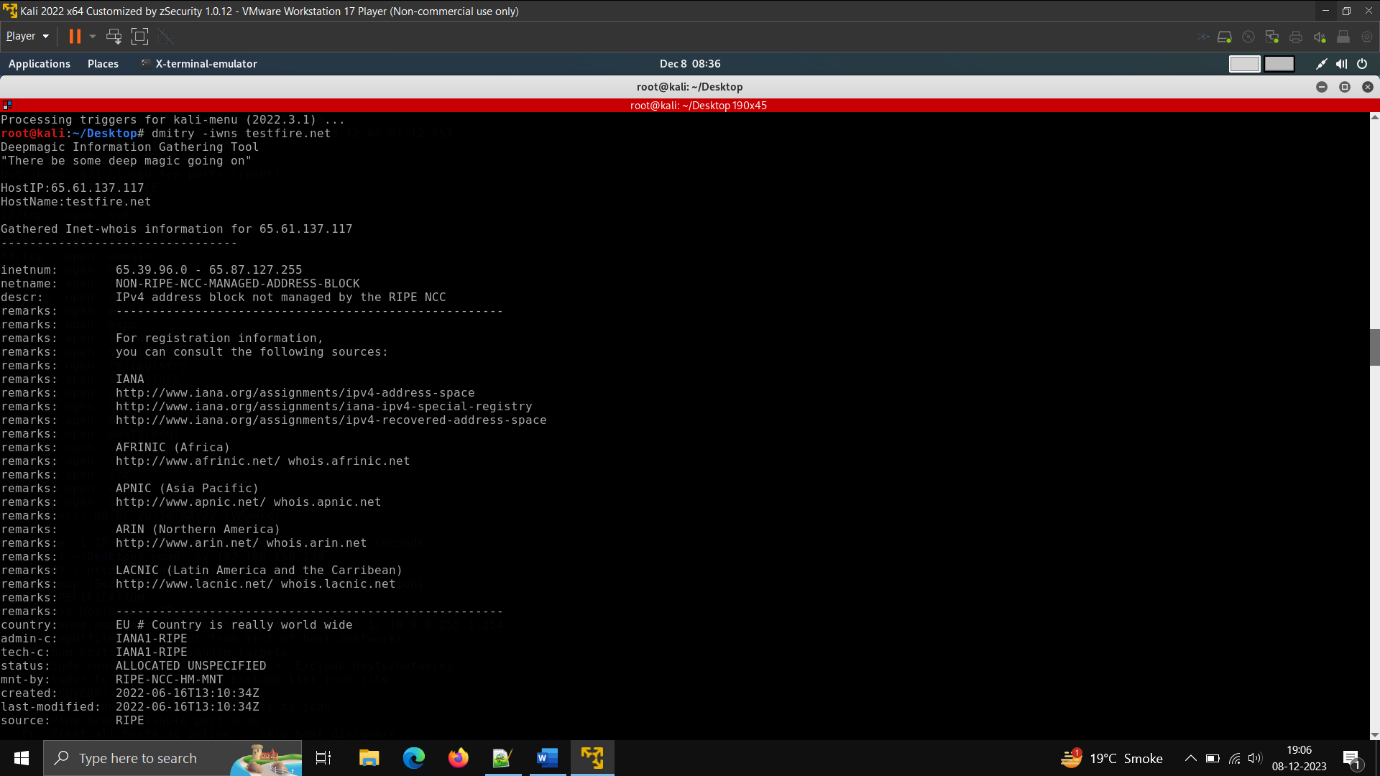


**nmap command – used for port scanning and no of host available in network.**

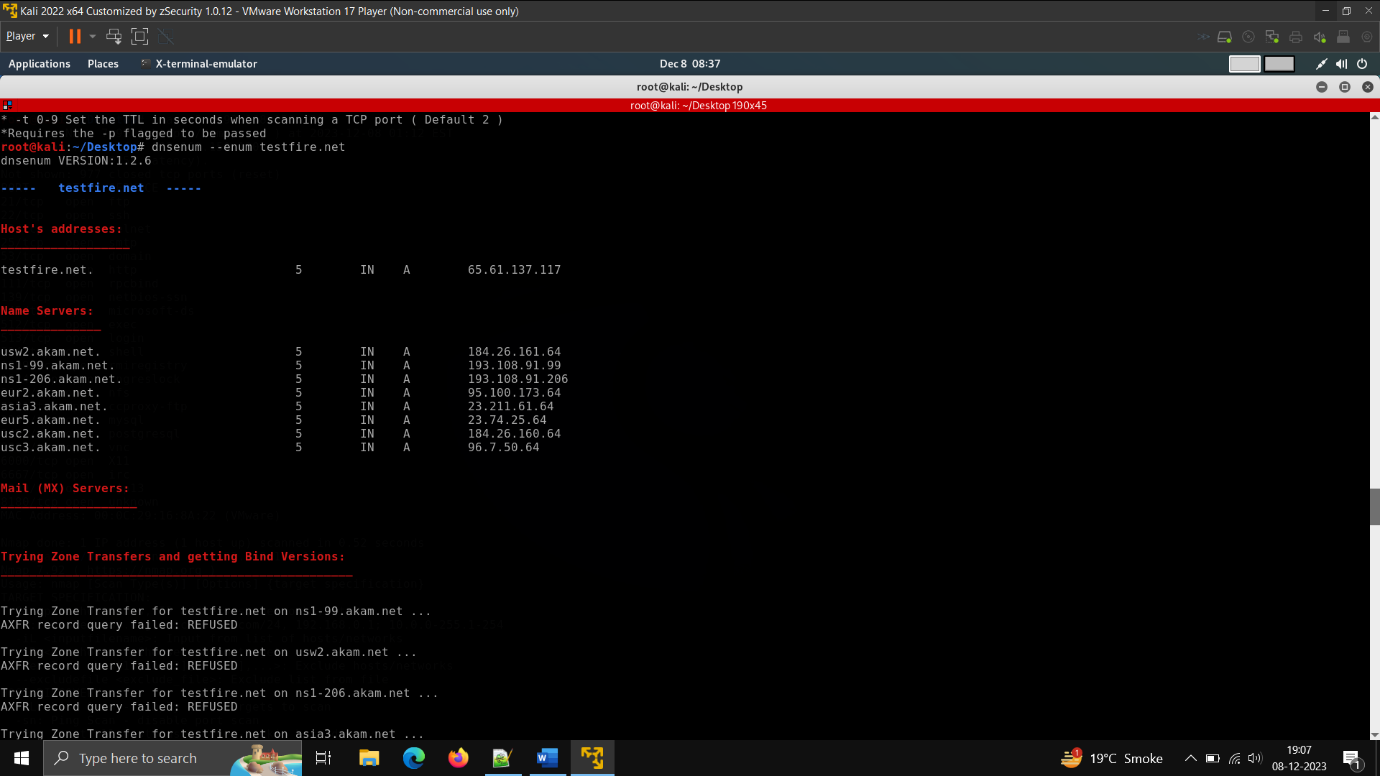


**Nmap -sV ,Nmap -Pn**

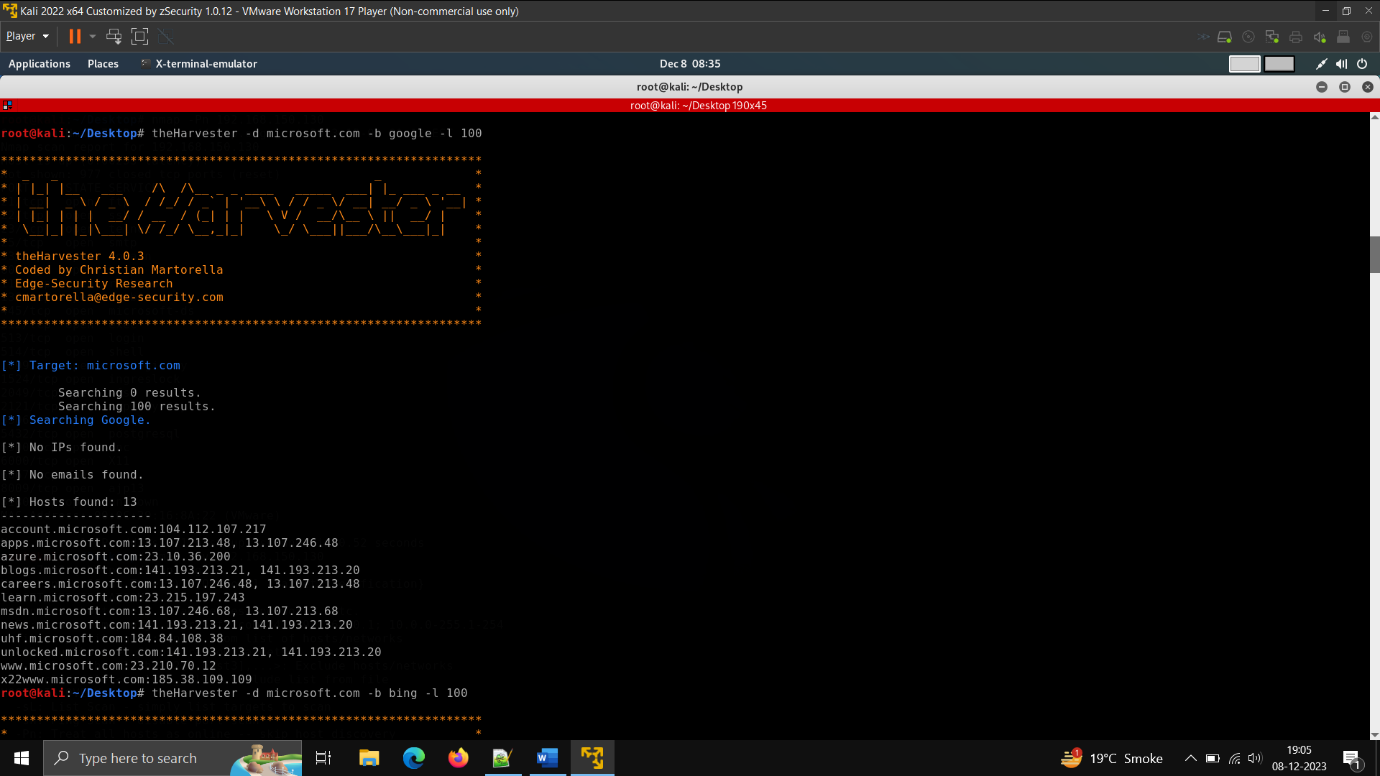
**Used -Pn in case of disabling ping and -sV in case of getting version for checking exploits**



**Dmitry command(info gathering)**

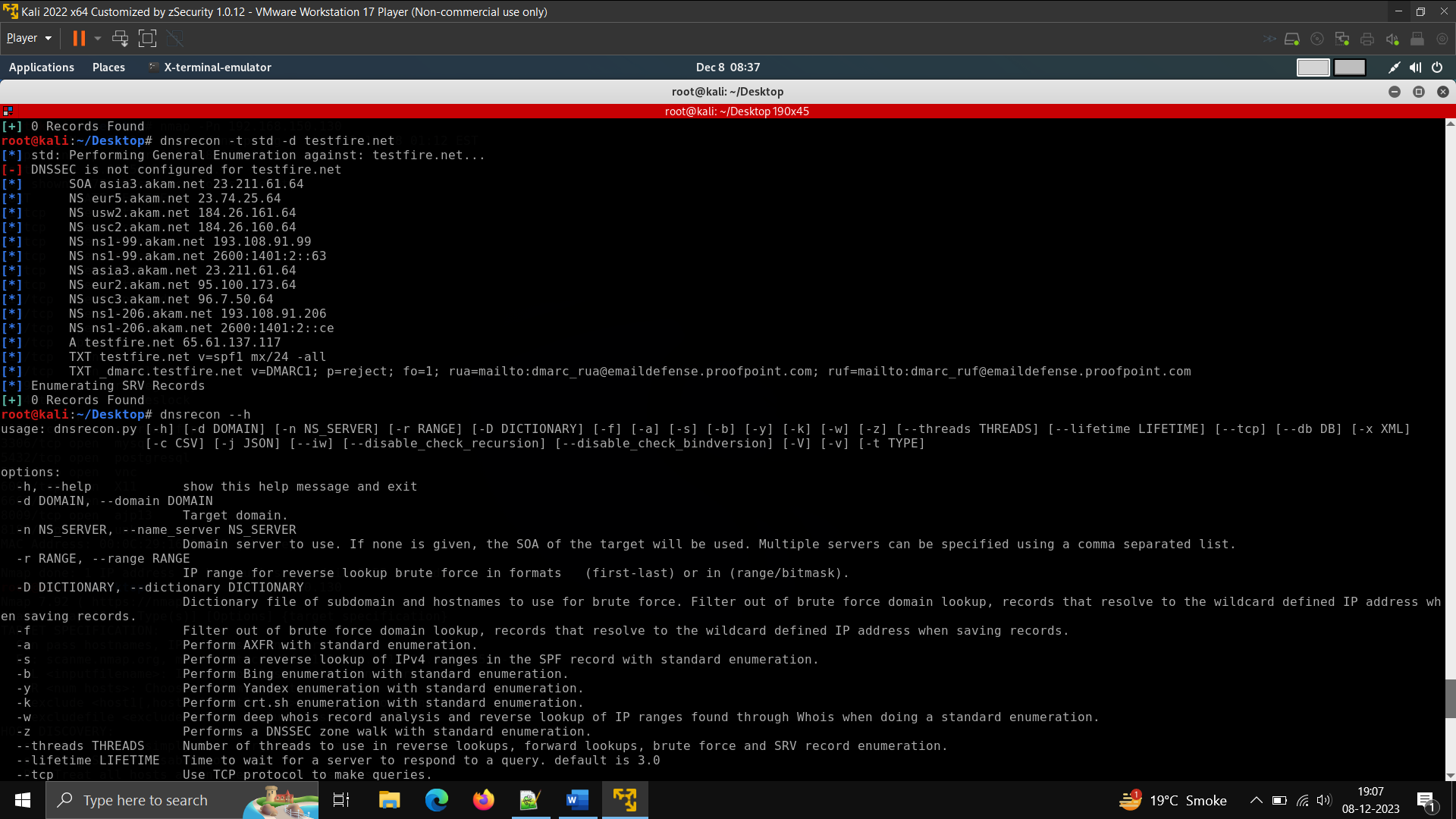


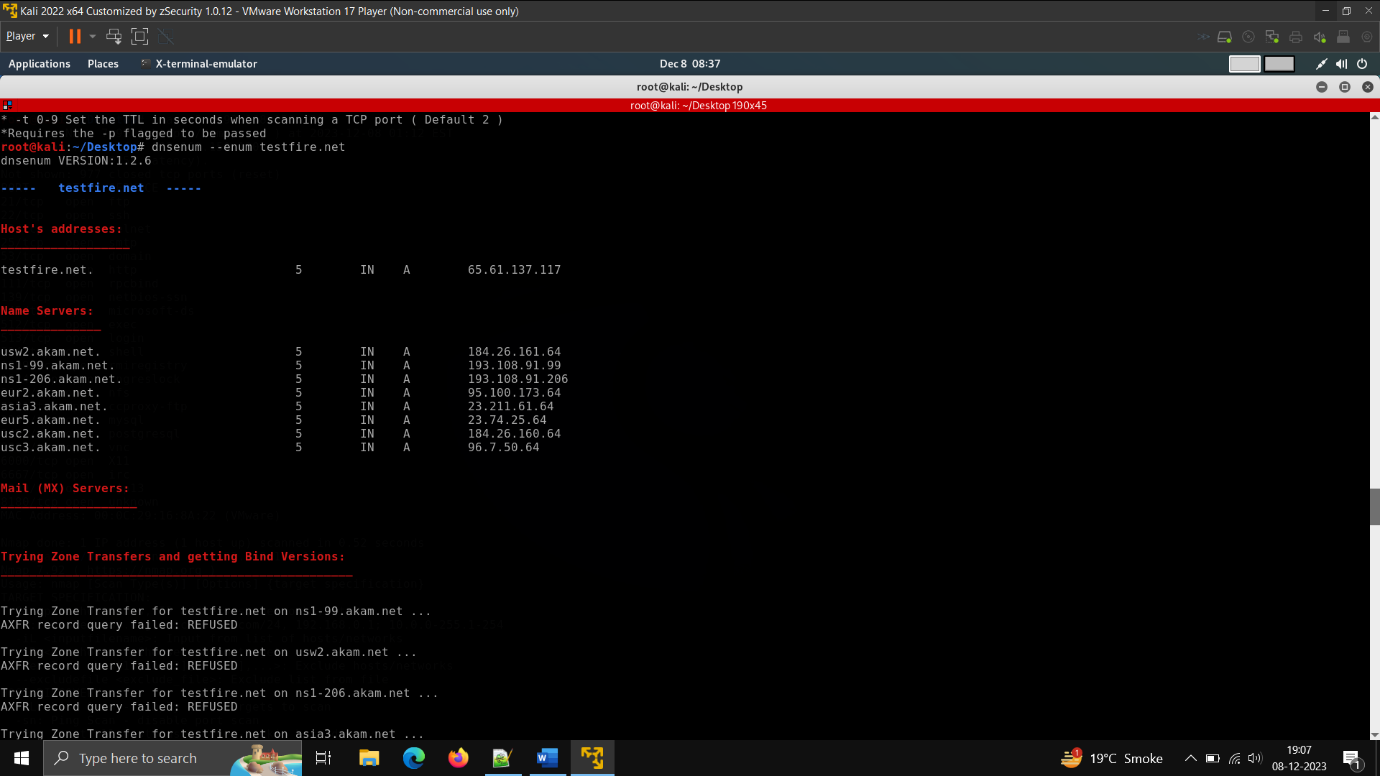
**Dnsenum command**



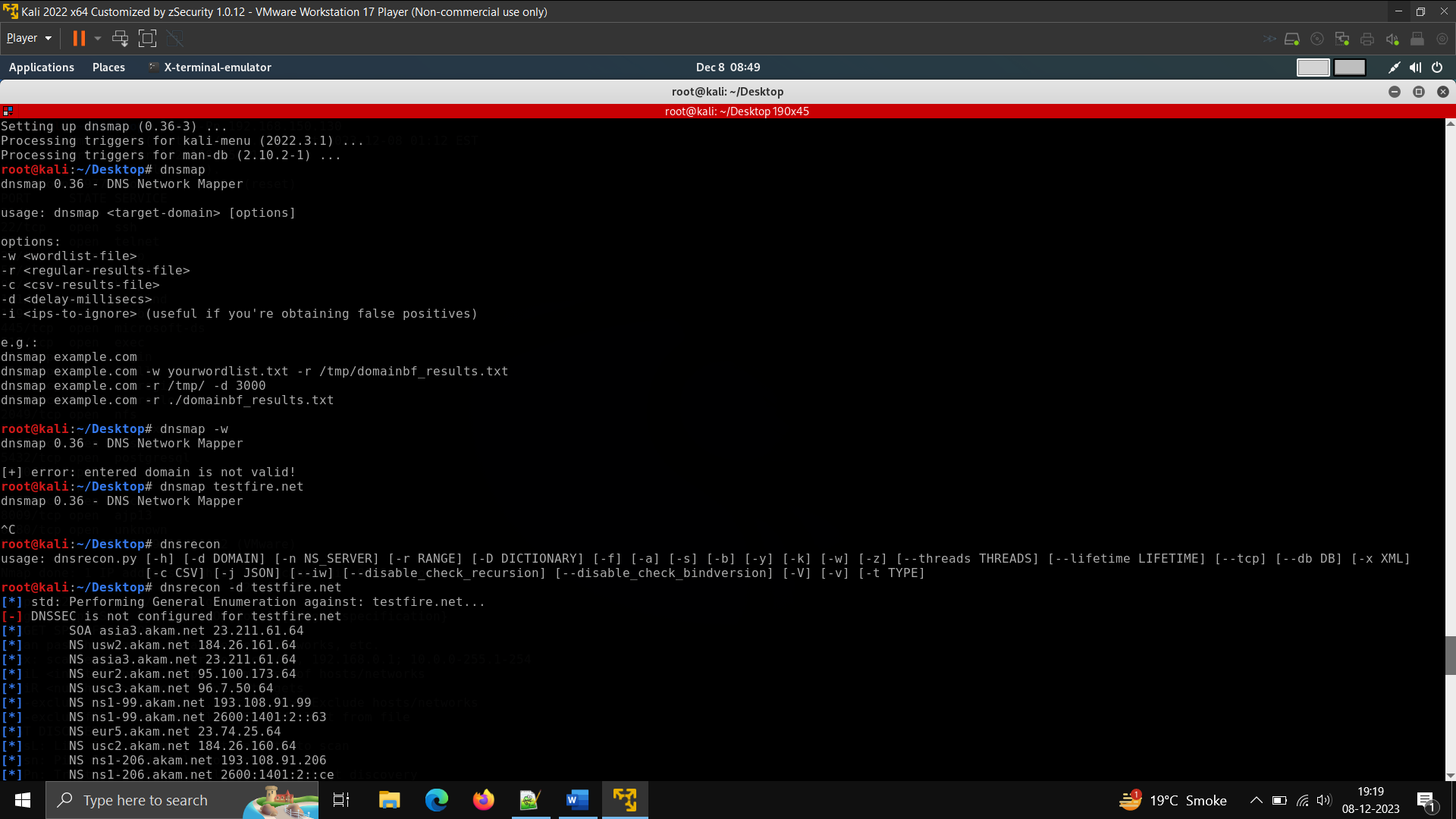
**theHarvester command –(similar to netcraft)**

**Dnsrecon command**



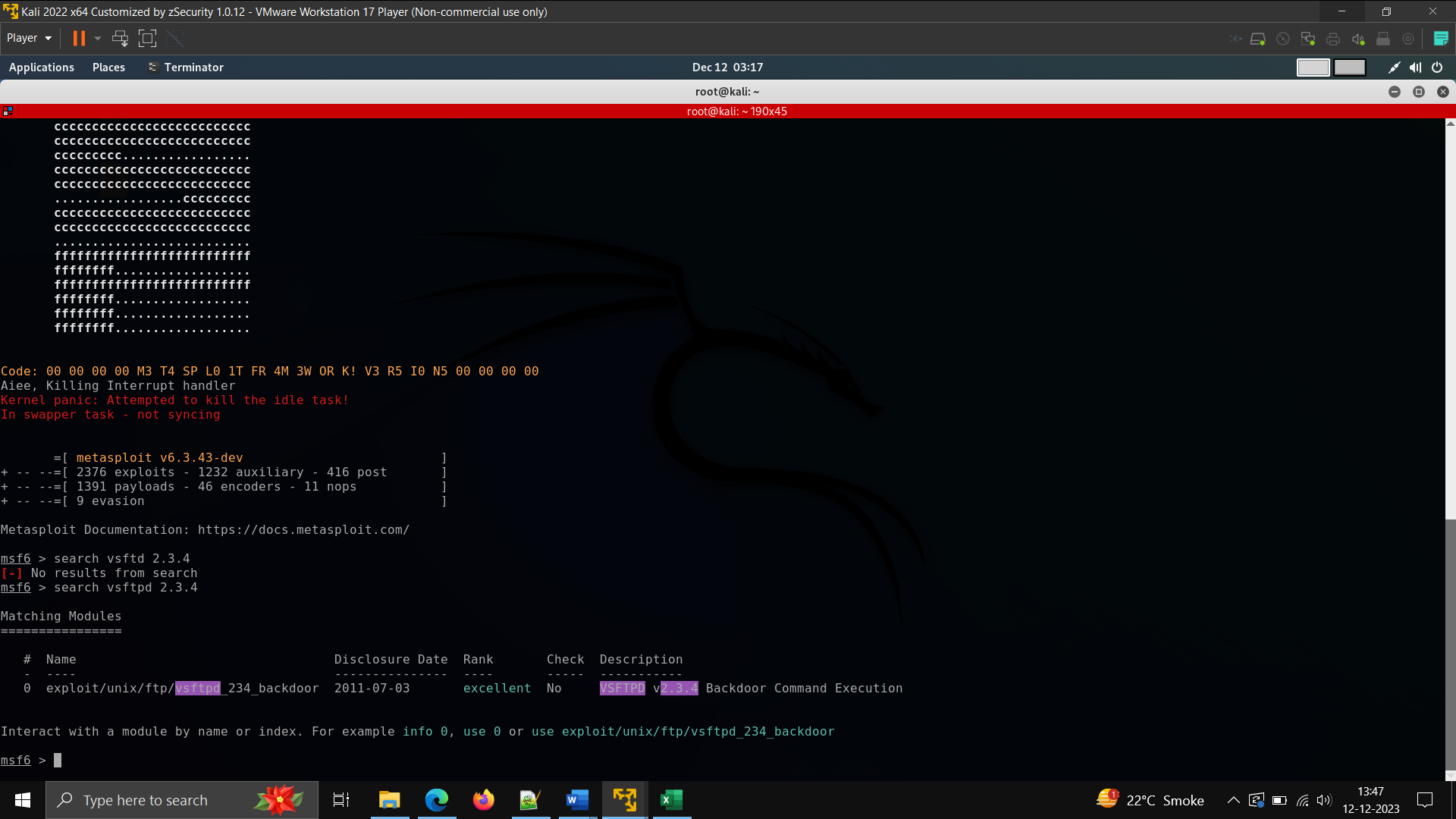


**Dnsmap command**



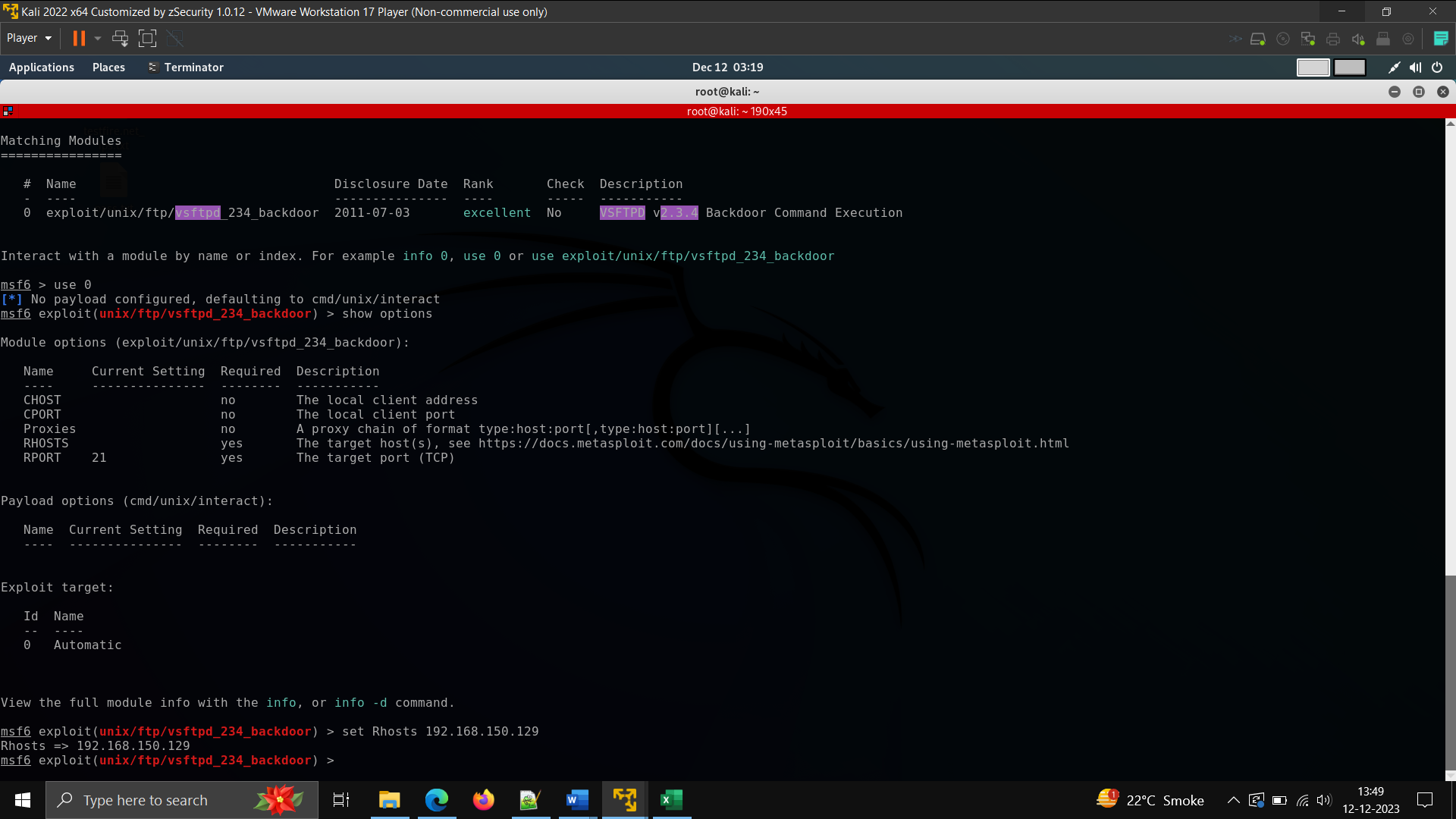
**Metasploit – use msfconsole to start -checking for vsftpd 2.3.4**

**search vsftpd 2.34**

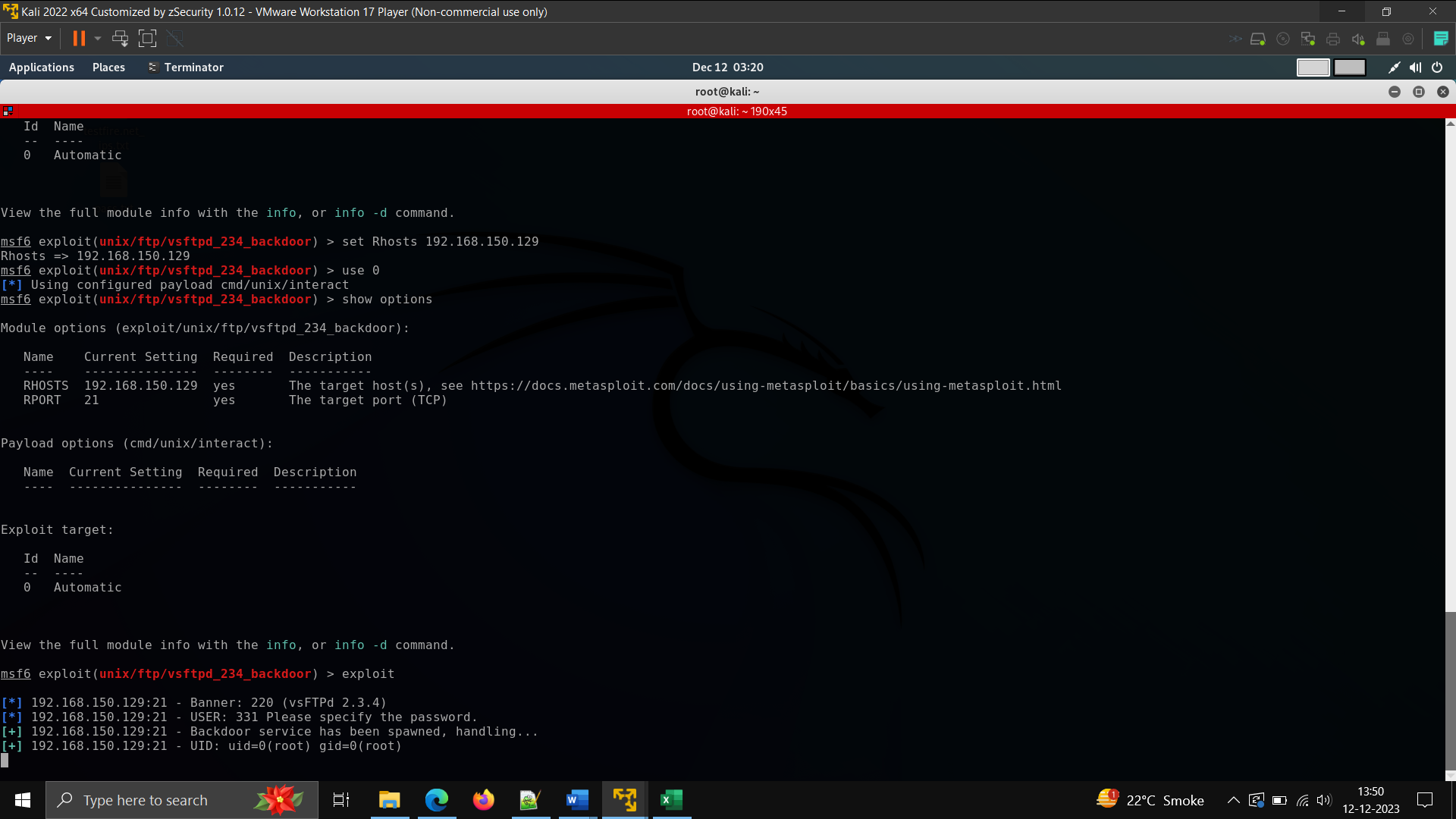


**Use 0 – it will say payload not configure**

**Then check – show options and configure only RHOStS to target IP as it is mandatory to set.**



**Then use command -exploit –**



**Now ftp is given a remote shell to communicate, in etc/passwd use the hash file to decrypt the hashes.**

**You can also login again by checking the session-i and also using ftp target IP**

**Possible remediation –**

* **Use strong password that takes time to break**
* **Regular change password**
* **Use firewall to configure request**
* **Use IDS system to detect malicious attacks**
* **Patching software.**
* **Regular audit of the system.**