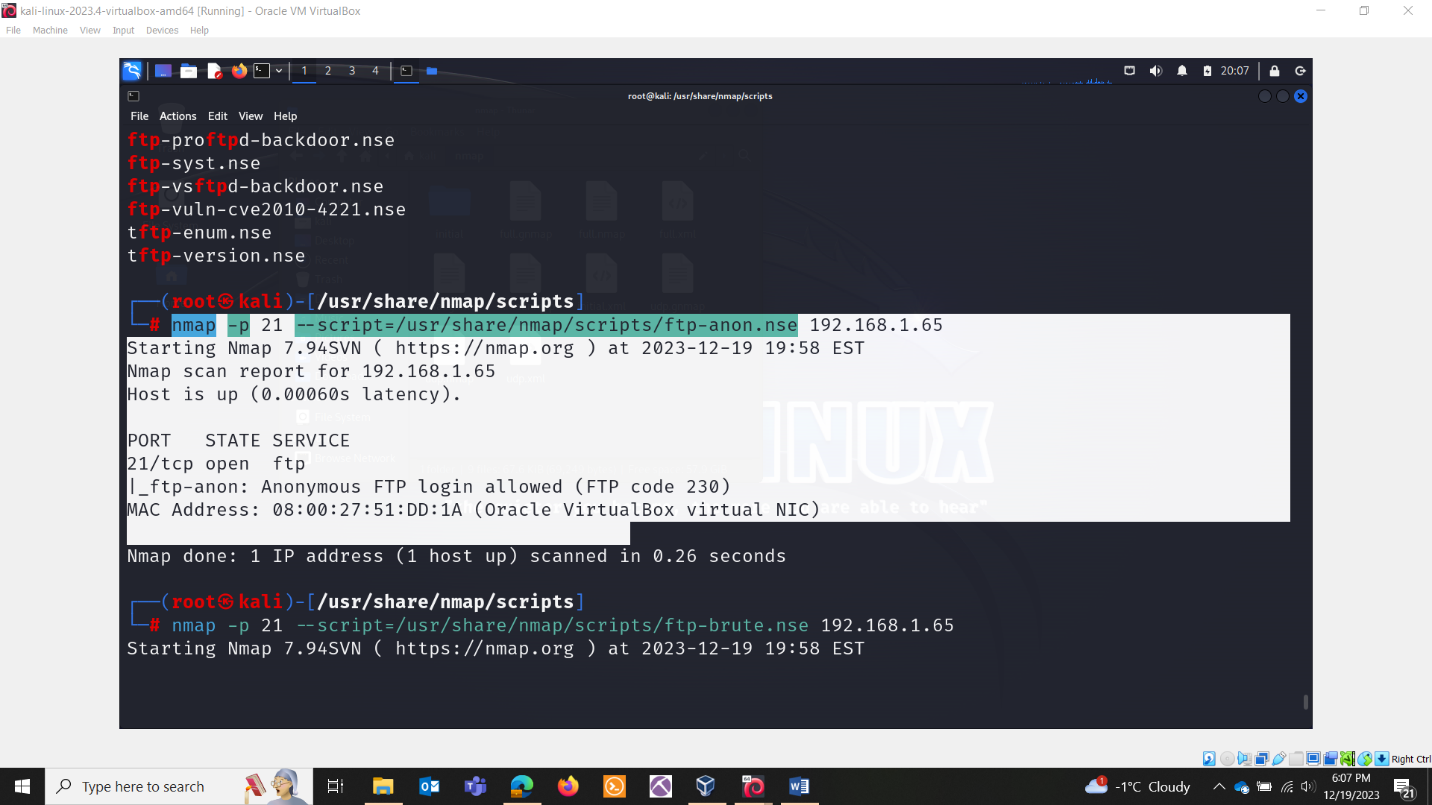
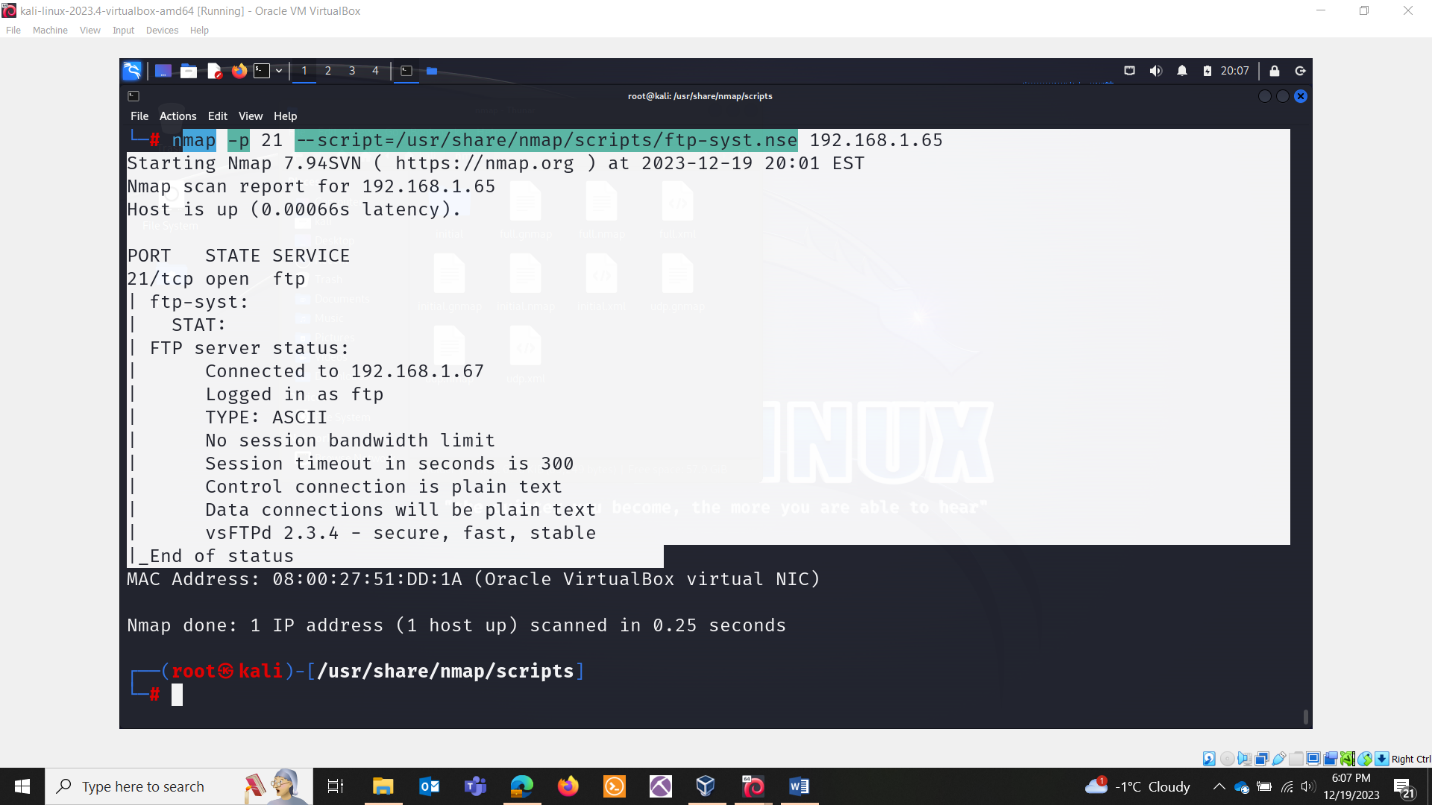
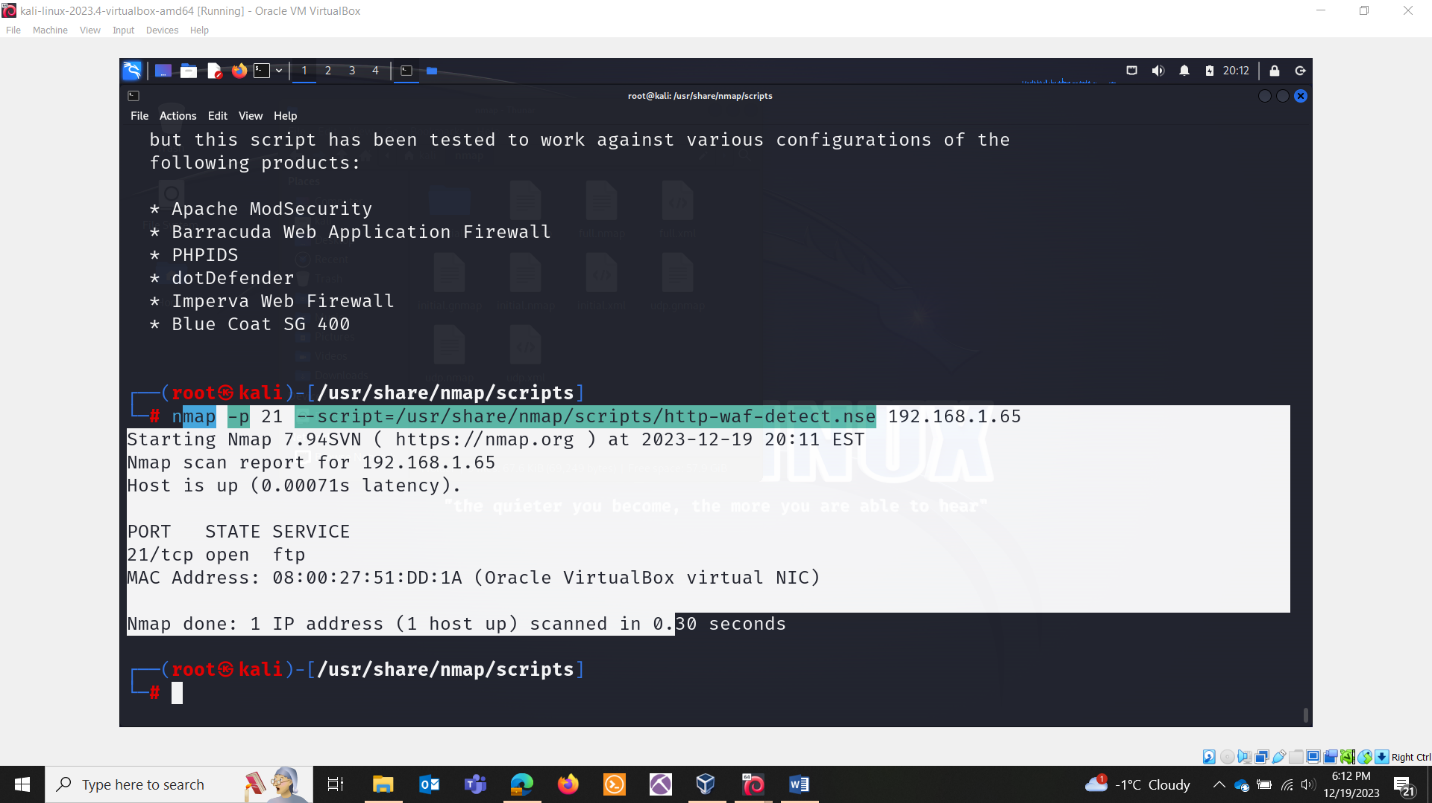
**NMAP SCRIPT**

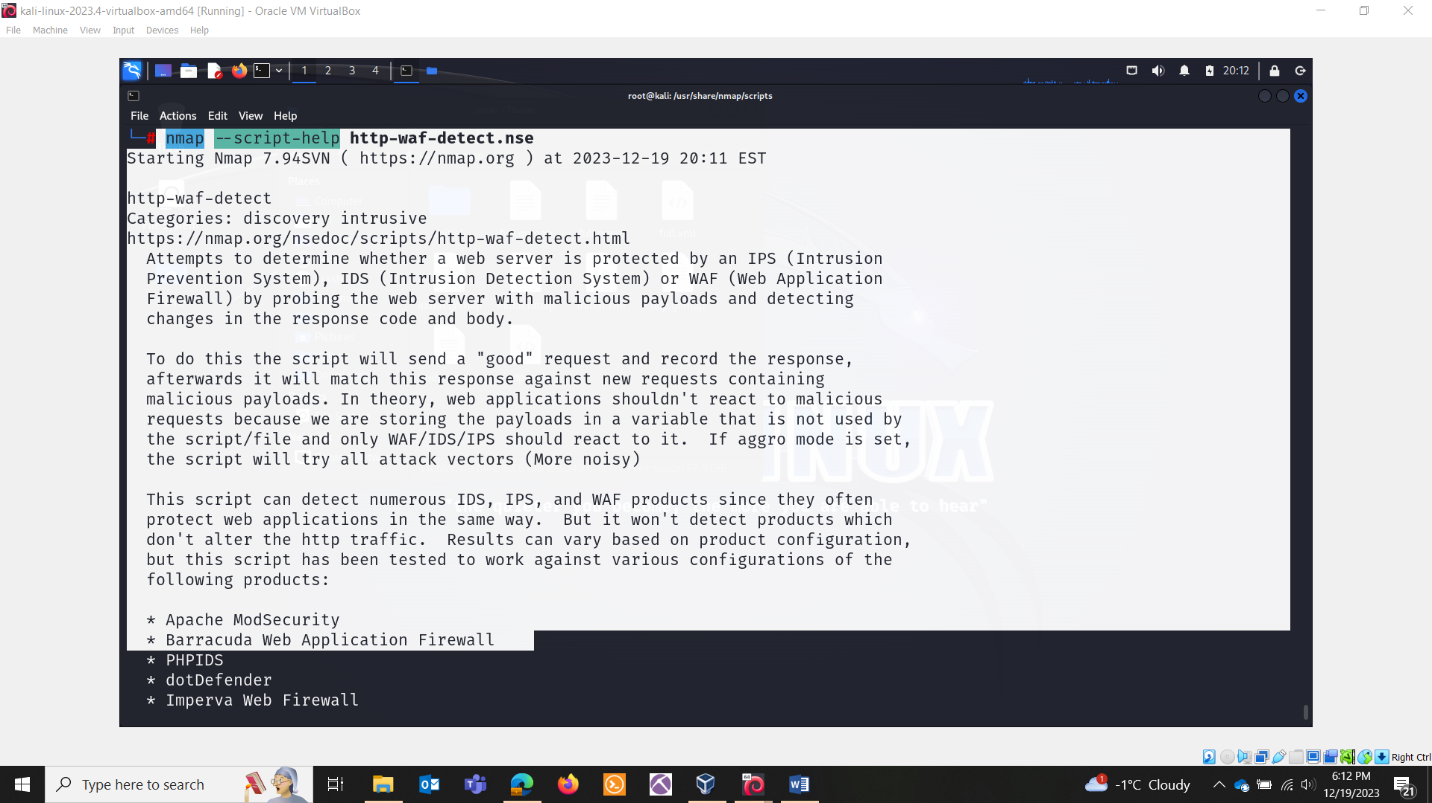
[Nmap Scripts - OSCP Playbook (gitbook.io)](https://fareedfauzi.gitbook.io/oscp-playbook/port-scanning/nmap-scripts)

* Scripts are present in /usr/share/nmap/scripts





Help with scripts.



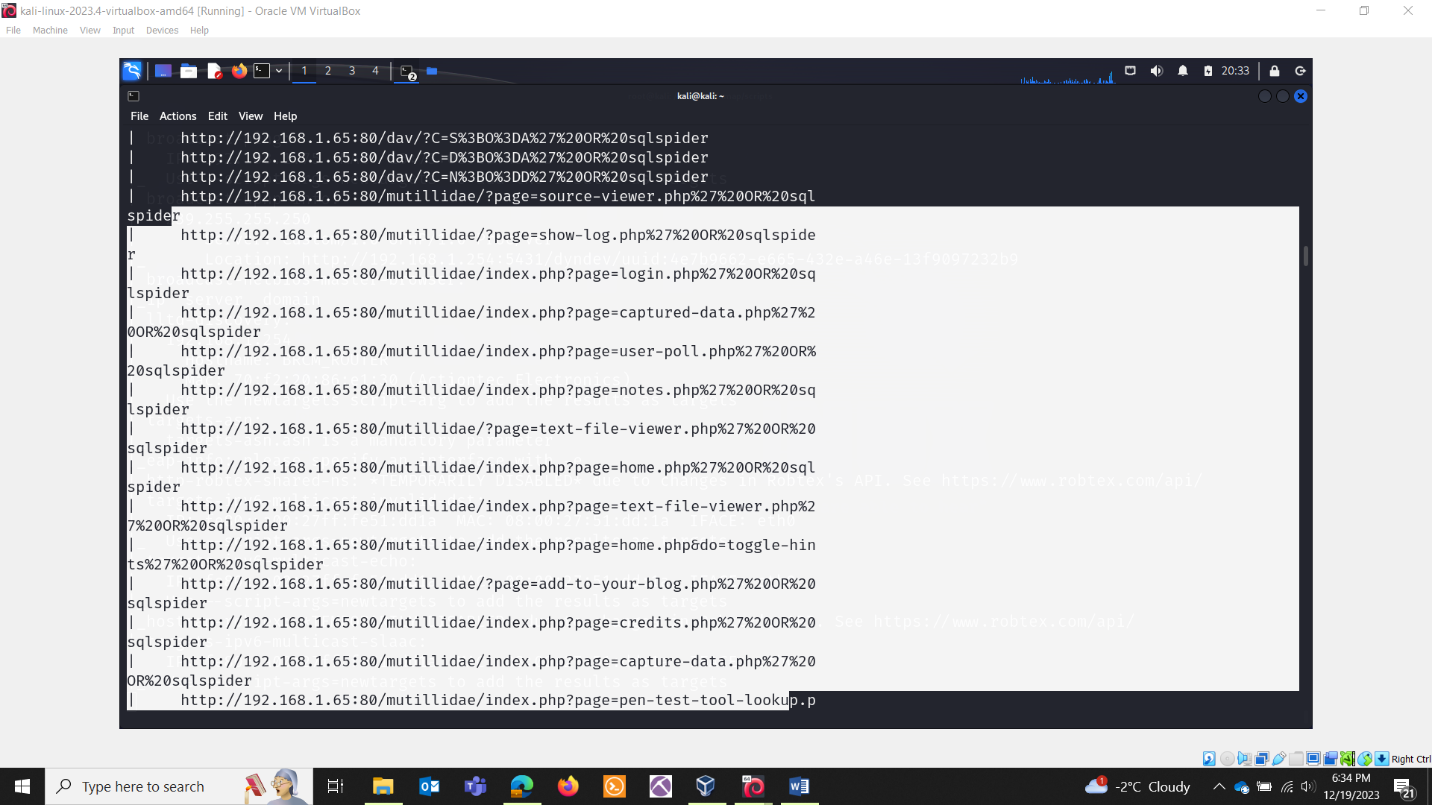
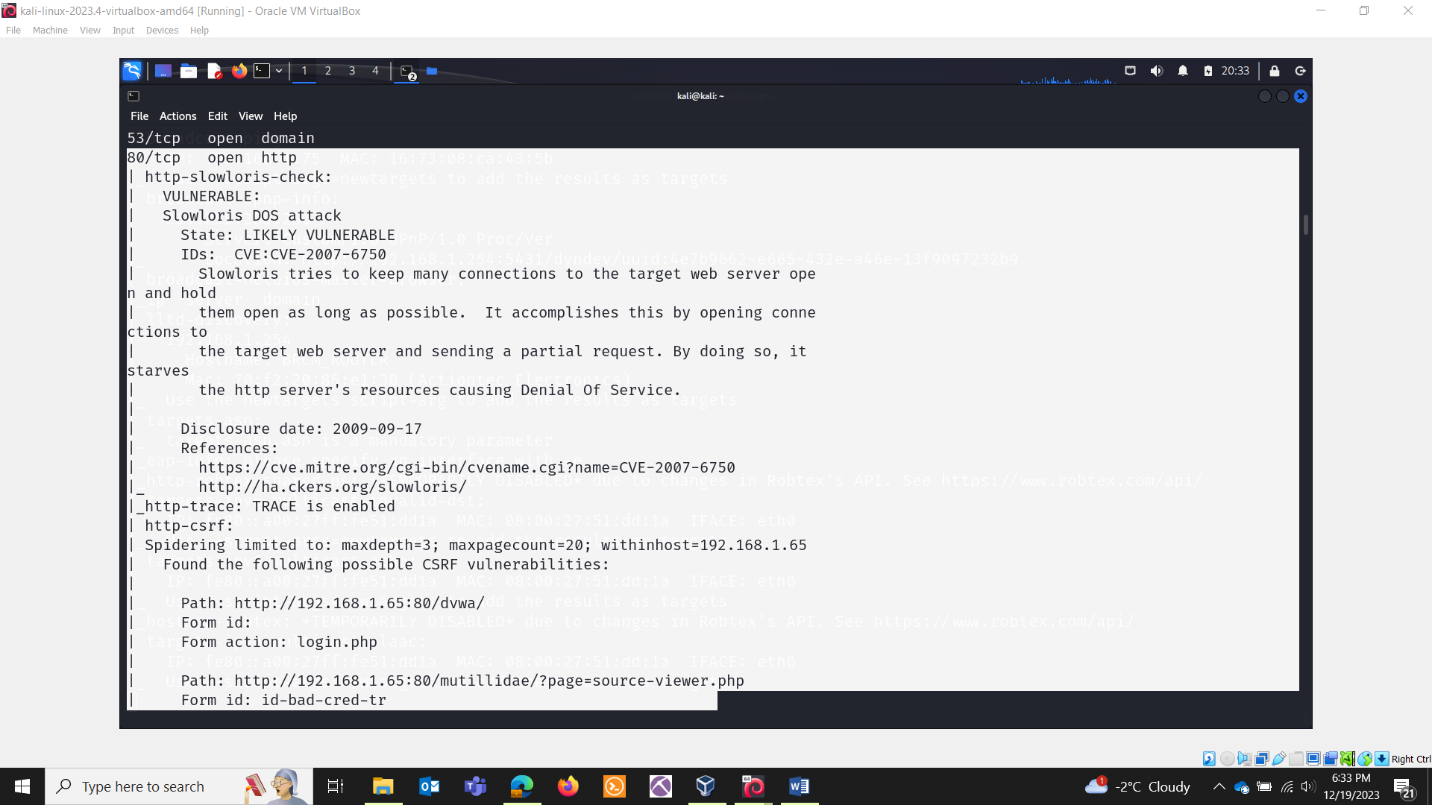
VULNERABILITY SCANNING WITH NMAP SCRIPTS:

Vulnerability scripts, in the context of security tools like Nmap's NSE (Nmap Scripting Engine) or other security scanners, refer to scripts designed to identify and exploit vulnerabilities in target systems. These scripts are often used in penetration testing, ethical hacking, and security assessments to discover and analyze potential weaknesses in a network or system.

Nmap's NSE, for example, includes a wide range of scripts that can be used to detect and exploit vulnerabilities in various services and applications. These scripts are categorized as "vuln" scripts and are typically named in a way that reflects the type of vulnerability they target.

Here are a few examples of Nmap vuln scripts:

* http-vuln-\* scripts: Scripts targeting vulnerabilities in web applications and servers.
* smb-vuln-\* scripts: Scripts targeting vulnerabilities in SMB (Server Message Block) services, commonly used in Windows environments.
* ftp-vuln-\* scripts: Scripts targeting vulnerabilities in FTP (File Transfer Protocol) services.
* pop3-vuln-\* scripts: Scripts targeting vulnerabilities in POP3 (Post Office Protocol) email services.
* ssl-vuln-\* scripts: Scripts targeting vulnerabilities in SSL/TLS (Secure Sockets Layer/Transport Layer Security) protocols.



Target scan with all the scripts:

