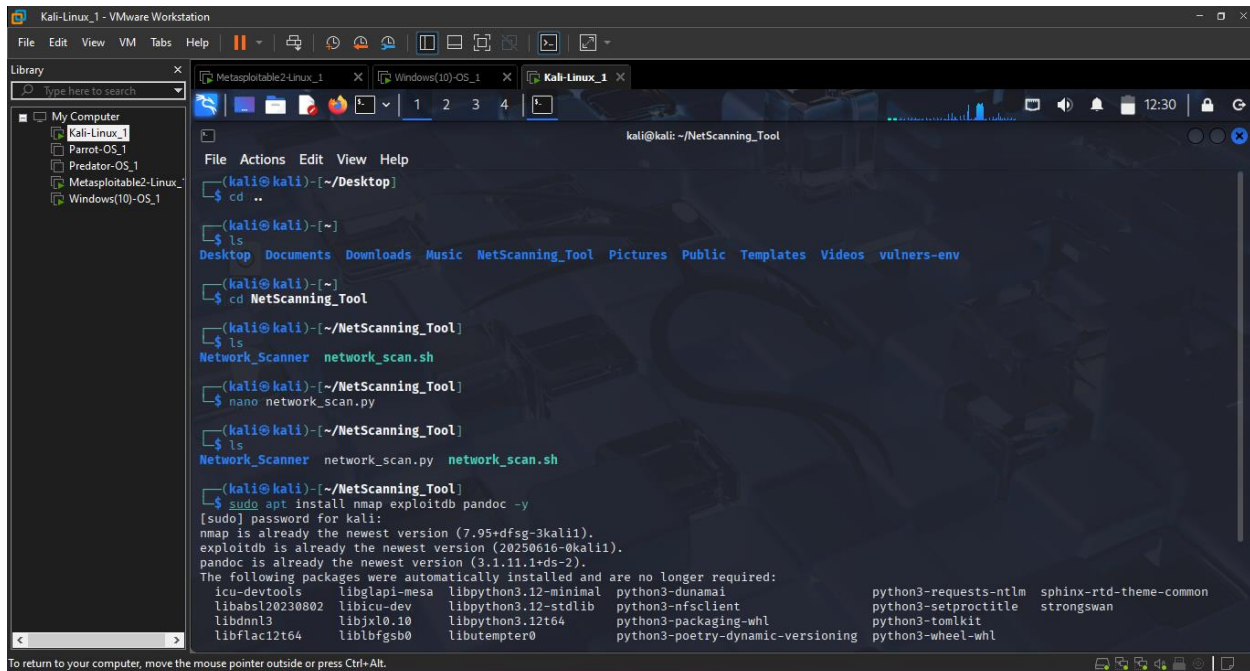
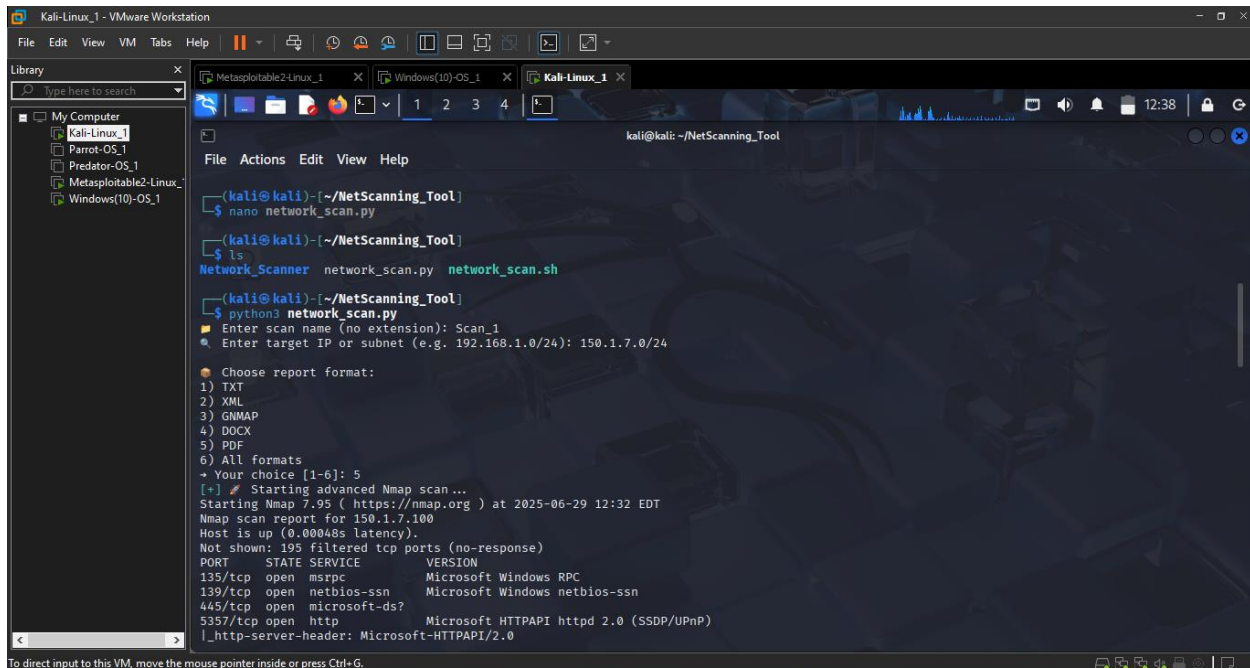


Network Scanner Screenshots



This screenshot shows the initial setup of the NetScanning_Tool directory in a Kali Linux terminal. The user navigates to the Desktop, then to the NetScanning_Tool directory, and lists the files. The files listed are Network_Scanner, network_scan.sh, and network_scan.py. The user then runs the command `sudo apt install nmap exploitdb pandoc -y` to install the necessary tools. The output shows that nmap and exploitdb are already the newest versions, and pandoc is already the newest version. The following packages were automatically installed and are no longer required: libicu-devtools, libglapi-mesa, libpython3.12-minimal, python3-dunamai, python3-requests-ntlm, sphinx-rtd-theme-common, libabsl20230802, libicu-dev, libpython3.12-stdlib, python3-nfsclient, python3-setproctitle, strongswan, libdnnl3, libjxl0.10, libpython3.12t64, python3-packaging-whl, python3-tomlkit, libflac12t64, liblbfgsb0, libutempter0, python3-poetry-dynamic-versioning, and python3-wheel-whl.

```
kali@kali: ~/NetScanning_Tool
File Actions Edit View Help
(kali@kali)~-[~/Desktop]
$ cd ..
(kali@kali)~-[~]
$ ls
Desktop Documents Downloads Music NetScanning_Tool Pictures Public Templates Videos vulners-env
(kali@kali)~-[~]
$ cd NetScanning_Tool
(kali@kali)~-[~/NetScanning_Tool]
$ ls
Network_Scanner network_scan.sh
(kali@kali)~-[~/NetScanning_Tool]
$ nano network_scan.py
(kali@kali)~-[~/NetScanning_Tool]
$ ls
Network_Scanner network_scan.py network_scan.sh
(kali@kali)~-[~/NetScanning_Tool]
$ sudo apt install nmap exploitdb pandoc -y
[sudo] password for kali:
nmap is already the newest version (7.95+dfsg-3kali1).
exploitdb is already the newest version (20250616-0kali1).
pandoc is already the newest version (3.111.1+ds-2).
The following packages were automatically installed and are no longer required:
libicu-devtools libglapi-mesa libpython3.12-minimal python3-dunamai python3-requests-ntlm sphinx-rtd-theme-common
libabsl20230802 libicu-dev libpython3.12-stdlib python3-nfsclient python3-setproctitle strongswan
libdnnl3 libjxl0.10 libpython3.12t64 python3-packaging-whl python3-tomlkit
libflac12t64 liblbfgsb0 libutempter0 python3-poetry-dynamic-versioning python3-wheel-whl
```



This screenshot shows the execution of the network_scan.py script in a Kali Linux terminal. The user runs the command `python3 network_scan.py`. The script prompts the user to enter a scan name (no extension) and a target IP or subnet (e.g. 192.168.1.0/24). The user enters 'Scan_1' and '150.1.7.0/24'. The script then prompts the user to choose a report format. The user chooses '5' (PDF). The script then starts an advanced Nmap scan. The output shows the scan results for 150.1.7.100. The scan is up (0.00048s latency). Not shown: 195 filtered tcp ports (no-response). The scan results are as follows:

PORT	STATE	SERVICE	VERSION
135/tcp	open	msrpc	Microsoft Windows RPC
139/tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
445/tcp	open	microsoft-ds?	
5357/tcp	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)

The script also shows the http-server-header: Microsoft-HTTPAPI/2.0.

```
kali@kali: ~/NetScanning_Tool
File Actions Edit View Help
(kali@kali)~-[~/NetScanning_Tool]
$ nano network_scan.py
(kali@kali)~-[~/NetScanning_Tool]
$ ls
Network_Scanner network_scan.py network_scan.sh
(kali@kali)~-[~/NetScanning_Tool]
$ python3 network_scan.py
Enter scan name (no extension): Scan_1
Enter target IP or subnet (e.g. 192.168.1.0/24): 150.1.7.0/24
Choose report format:
1) TXT
2) XML
3) GNMAP
4) DOCX
5) PDF
6) All formats
Your choice [1-6]: 5
[+] # Starting advanced Nmap scan ...
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-29 12:32 EDT
Nmap scan report for 150.1.7.100
Host is up (0.00048s latency).
Not shown: 195 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds?
5357/tcp   open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
_http-server-header: Microsoft-HTTPAPI/2.0
```

Kali-Linux_1 - VMware Workstation

File Edit View VM Tabs Help

Library

My Computer

- Kali-Linux_1
- Parrot-OS_1
- Predator-OS_1
- Metasploitable2-Linux_1
- Windows(10)-OS_1

Metasploitable2-Linux_1 Windows(10)-OS_1 Kali-Linux_1

1 2 3 4

kali@kali: ~/NetScanning_Tool

```
GNU nano 8.4 network_scan.py
import os
import subprocess
from datetime import datetime
from shutil import which

# -- Setup Directories --
BASE_DIR = "Network_Scanner"
LOG_DIR = os.path.join(BASE_DIR, "python_logs")
os.makedirs(LOG_DIR, exist_ok=True)

def green(msg): print(f"\033[92m+\033[0m {msg}")
def yellow(msg): print(f"\033[93m*\033[0m {msg}")
def red(msg): print(f"\033[91m!\033[0m {msg}")

# -- Tool Check --
def check_tools():
    for tool in ["nmap", "searchsploit"]:
        if which(tool) is None:
            red(f"{tool} is not installed. Please install it.")
            exit(1)
        if which("pandoc") is None:
            yellow("Pandoc not found: DOCK/PDF export will be skipped.")

check_tools()

# -- Get Scan Info --
filename = input("\U0001F4C1 Enter scan name (no extension): ").strip()
timestamp = datetime.now().strftime("%Y%m%d_%H%M%S")
```

Read 138 lines

Ctrl-H Help Ctrl-O Write Out Ctrl-W Where Is Ctrl-X Exit Ctrl-R Read File Ctrl-N Replace Ctrl-V Paste Ctrl-E Execute Ctrl-L Location Ctrl-G Go To Line Ctrl-U Undo Ctrl-M Set Mark Ctrl-C Copy Ctrl-T To Bracket Ctrl-F Where Was

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.