#!/bin/bash

# run with: ./NewBox.sh

# Set the NAME and IP variables

echo -n "What is the name of the new box?: "

read Box

echo -n "What is the IP address of $Box?: "

read IP

echo $(IP=$IP)

# Make folder for work to go and move into it...

mkdir ./$Box

cd $Box

# Make folders for notes and scans etc.

mkdir Scans Scans/Nmap Scans/Dirs Resources Resources/ScreenShots Resources/Scripts

# Create notes file and open

echo "# $Box $IP" > $Box.md

echo " " >> $Box.md

echo "# Enummeration" >> $Box.md

echo " " >> $Box.md

echo "# Resources" >> $Box.md

echo " " >> $Box.md

echo "# Exploits" >> $Box.md

echo " " >> $Box.md

echo "# PostEx Enum" >> $Box.md

echo " " >> $Box.md

echo "# PrivEsc" >> $Box.md

echo " " >> $Box.md

echo "# Notes" >> $Box.md

echo " " >> $Box.md

echo "## End ##" >> $Box.md

touch "$Box.Outline.md"

echo "# $Box $IP" > "$Box.Outline.md"

echo " " >> $Box.Outline.md

echo "# Enummeration" >> $Box.Outline.md

echo " " >> $Box.Outline.md

echo "# Resources" >> $Box.Outline.md

echo " " >> $Box.Outline.md

echo "# Exploits" >> $Box.Outline.md

echo " " >> $Box.Outline.md

echo "# PostEx Enum" >> $Box.Outline.md

echo " " >> $Box.Outline.md

echo "# PrivEsc" >> $Box.Outline.md

echo " " >> $Box.Outline.md

echo "## End ##" >> $Box.Outline.md

# Open MD files to begin note taking.

subl $Box.md

subl "$Box.Outline.md"

# Make Scan folder and start scanning...

cd Scans/Nmap

sudo nmap -sV -Pn -T4 -vv -oX sheet.xml -oN Nmap $IP

# Test script with this nmap scan...

# and make sure to comment out all other

# nmap scans...

# sudo nmap -sn -T4 -oN Nothing $IP

echo " "

echo " "

echo "...Now take a breath..."

sleep 10

echo " "

echo " "

echo "...finishing up..."

sleep 10

echo " "

echo " "

echo "...One more scan..."

echo " "

echo " "

# Test script with this nmap scan...

# sleep 5 && sudo nmap -sn -T4 -oN Nothing2 $IP

sleep 5 && sudo nmap -O -Pn -T4 -vv -oN Fingerprint -oX Fingerprint.xml $IP

echo " -----------------------------------------------------------------"

echo " Directories made, scans started, EXPLOIT $IP!!! "

echo " Save everything, screenshot it all! Try Harder!!! "

echo " -----------------------------------------------------------------"

echo " "

echo " "

xsltproc sheet.xml -o Nmap.html

xsltproc Fingerprint.xml -o Fingerprint.html

sudo chmod -R 766 $Box

sleep 2

echo "\*\*\* Start Hacking!!! \*\*\*"

#--Now you can start your other scans