Security Assessment and Operations Lab

Exercise 1 - Scanning and Enumeration SS 2023

Introduction

In this exercise the very first step of active scanning will be practiced, the network enumeration. Enumeration starts with host discovery, where hosts on the network are identified by enumerating the hosts that respond to TCP or ICMP requests. The next step is port scanning where all the open ports on a target are enumerated. To make an assumption about possible vulnerabilities, the services and respective versions are determined by testing whether the TCP ports are open. Banner grabbing and OS fingerprinting on the host may also be helpful for finding vulnerabilities. In this Lab we will be using Kali Linux, as mentioned in the preparation guide. You also need to connect to the lab network over a VPN connection. To do this download the VPN Pack for your group in OLAT. If you are stuck during the exercises, do not hesitate to contact Daniel Reti.

```
$ ip route
0.0.0.0/1 via 10.9.0.5 dev tun0
default via 10.0.2.2 dev eth0 proto dhcp src 10.0.2.15 metric 100
10.0.2.0/24 dev eth0 proto kernel scope link src 10.0.2.15 metric 100
10.9.0.1 via 10.9.0.5 dev tun0
10.9.0.5 dev tun0 proto kernel scope link src 10.9.0.6
128.0.0.0/1 via 10.9.0.5 dev tun0
131.246.195.218 via 10.0.2.2 dev eth0
192.168.57.0/24 via 10.9.0.5 dev tun0
```

Listing 1: Finding your group's lab subnet after connecting to the VPN

Exercise 1-1: Ping Sweep and Port Scan

1. You must write a shell script that performs a ping sweep on your subnet. Some machines might not react to ICMPv4 messages, so you must find a way around this. We will provide you with a template, but you can also implement the script from scratch. You can find the template uploaded to Olat.
2. Use the nmap tool, preinstalled on Kali Linux, to perform a scan on the subnet.
3. Compare your results of your bash script and the nmap scan. Bonus: you can compare the probes with wireshark.
4. Use nmap to perform a port scan of the full TCP port range, a service scan and an OS fingerprint scan with the commands introduced in the lecture.

```
#!/bin/bash

check_host_alive_ping()
{
  <<< Insert ping command here >>>
  [ $? -eq 0 ] && echo 192.168.56.\$i
}

ips=($(for i in {1..254}; \
        do (check_host_alive_ping 192.168.56.$i & disown); done))

check_host_alive_???(){
  <<< Insert alternative command here >>>
}

ips+=($(for i in {1..254}; \
        do (check_host_alive_??? 192.168.56.$i & disown); done))
sorted_unique_ips= \
        ($(echo "${ips[@]}" | tr ' ' '\n' | sort -u | tr '\n' ' '))
#echo "${sorted_unique_ips[@]}"

check_host_port(){
    nc -nvz $1 1-100 > $1.txt 2>&1
    cat $1.txt
    rm -rf \$1.txt
}

for i in "${sorted_unique_ips[@]}"; do (check_host_port $i); done
```

Exercise 1-2: Directory Scan

This task will require you to write a small Python script (other languages are allowed as well) to scan subdirectories on the identified http service (also known as directory brute force or directory fuzzer). We will provide you with a wordlist to find the most common directories and files.

1. Identify which directories are present using a http library and the wordlist
2. Search for files in the root path and in the directories from step 1. Use the file extensions `.html,` `.php`, and `.txt`.

Perform a gobuster, dirbuster or similar tool scan as a comparison to your implementation.

Exercise 1-3: Find Flags

Find six flags hidden in different services on the lab machines you identified by interacting with these services. To give you a small hint to know what to look out for:

- Flag 1: SSH
- Flag 2: PHP Login Page
- Flag 3: HTML
- Flag 4: Hidden in a subdirectory
- Flag 5: FTP
- Flag 6: Samba

You can submit the flags you found through Olat. There will be a test with unlimited tries, so don't worry about getting it wrong.

Report

Write a brief report including your solutions and your findings across all six machines. Then, submit the report via Olat. You can find a LaTeXtemplate on OLAT.