Acceptance clause: by completing this project the student accepts that he/she is responsible for what he/she will do and that he/she will not use these tools outside the virtual one created for that purpose. The student also accepts the legal repercussions that some of these actions may be subject to if these actions are carried out on external sites.

Project 3: Information Gathering (scanning)[1]

Level: 2

Difficulty: medium-easy

Objective: Install and analyze the indicated tools obtaining information about worker1 (DO NOT USE outside the virtual network).

Task: The student will have to collect information about the tools, install them from the Debian repository and use it on worker1 to analyze its functionality and extract information from the worker1 VM. The analysis will be complemented with a Vulnerability Scanning.

Recommended: Start with project 1 to learn about footprinting tools.

Scanning is another essential step, which is necessary, and it refers to the package of techniques and procedures used to identify hosts, ports, and various services within a network. Network scanning is one of the components of intelligence gathering and information retrieving mechanism an attacker used to create an overview scenario of the target organization (target organization: means the group of people or organization which falls in the prey of the Hacker). Vulnerability scanning is performed by pen-testers to detect the possibility of network security attacks. This technique led hackers to identify vulnerabilities such as missing patches, unnecessary services, weak authentication, or weak encryption algorithms. So a pen-tester and ethical hacker list down all such vulnerabilities found in an organization's network.

Scanning is of three types:

- Network Scanning
- Port Scanning
- Vulnerability Scanning

Objectives of network scanning:

- To discover live hosts/computer, IP address, and open ports of the victim.
- To discover services that are running on a host computer.
- To discover the Operating System and system architecture of the target.

1 Some parts are based on: https://www.w3schools.in/ethical-hacking

- To discover and deal with vulnerabilities in Live hosts.

Scanning Methodologies:

- Hackers and Pen-testers check for Live systems.
- Check for open ports (the technique is called Port Scanning, which will be discussed below)
- Scanning beyond IDS (Intrusion Detection System)
- Scan for vulnerability

Port Scanning: It is a conventional technique used by penetration testers and hackers to search for open doors from which hackers can access any organization's system. During this scan, hackers need to find out those live hosts, firewalls installed, operating systems used, different devices attached to the system, and the targeted organization's topology. Once the Hacker fetches the victim organization's IP address by scanning TCP and UDP ports, the Hacker maps this organization's network under his/her grab. **nmap/amap** are tool to perform port scanning.

TCP/IP Handshake: Before moving to the scanning techniques, we have to understand the 3-way TCP/IP handshaking process. In computer terms, handshaking means the automated process used to set dynamic parameters of a communication channel between two entities using some protocols. Here, TCP (Transmission Control Protocol) and IP (Internet Protocol) are the two protocols used for handshaking between a client and a server. Here first, the client sends a synchronization packet for establishing a connection, and the server listens to and responds with a syn/ack packet to the client. The client again responds to the server by sending an ack packet. Here SYN denotes synchronization, which is used to initialize connections between the client and the server in packets. ACK denotes acknowledgment, which is used to establish a connection between two hosts.

Scanning techniques mainly used:

- SYNScan: SYN scan or stealth doesn't complete the TCP three-way handshake technique. A hacker sends an SYN packet to the victim, and if an SYN/ACK frame is received back, then the target would complete the connection, and the port is in a position to listen. If an RST is retrieved from the target, it is assumed that the port is closed or not activated. SYN stealth scan is advantageous because a few IDS systems log this as an attack or connection attempt.
- XMASScan: XMAS scan send a packet which contains URG (urgent), FIN (finish) and PSH (push) flags. If there is an open port, there will be no response; but the target responds with an RST/ACK packet if the port is closed. (RST=reset).
- FINScan: A FIN scan is similar to an XMAS scan except that it sends a packet with just the FIN (finish) flag and no URG or PSH flags. FIN scan receives the same response and has the same limitations as XMAS scans.
- IDLEScan: An IDLE scan uses a spoofed/hoax IP to send the SYN packet to the target by determining the port scan response and IP header sequence number. Depending on the response of the scan, the port is determined, whether open or closed.

- Inverse TCP Flag Scan: Here, the attacker sends TCP probe packets with a TCP flag (FIN, URG PSH) or no flags. If there is no response, it indicates that the port is open, and RST means it is closed.
- ACK Flag Probe Scan: Here, the attacker sends TCP probe packets where an ACK flag is set to a remote device, analyzing the header information (TTL and WINDOW field). The RST packet signifies whether the port is open or closed. This scan is also used to check the target's/victim's filtering system.

Vulnerability Scanner:

It is the proactive identification of the system's vulnerabilities within a network in an automated manner to determine whether the system can be exploited or threatened. I this case, the computer should have to be connected to the internet.

Tools that can are used to scan networks and ports are:

- **nmap/nmapsi4:** extract information such as live hosts on the network, services, type of packet filters/firewalls, operating systems, and OS versions.
- **hping3:** are command-line packet crafting and network scanning tools used for TCP/IP protocols.
- **wireshark** and powerful and famous tool that listen to network traffic and act as network analyzers.
- Lynis: powerful tool for security auditing, compliance testing, and system hardening. Of course, you can also utilize this for vulnerability detection and penetration testing as well. It will scan the system according to the components it detects. For example, if it detects Apache – it will run Apache-related tests for pin point information.
- **pompem**: find exploit with a system of advanced search, designed to automate the search for Exploits and Vulnerability in the most important databases facilitating the work of pentesters, ethical hackers and forensics expert. Performs searches in databases: PacketStorm security, CXSecurity, ZeroDay, Vulners, National Vulnerability Database, WPScan Vulnerability Database. This tool is essential in the security of networks and systems.
- **vuls**: This is scanner which checks the package inventory against a local copy of the National Vunerabilities Database (NVD) of vulnerabilities according to their CVE (Common Vulnerabilities and Exposures) identifiers. The backends supports a couple of OSs (Debian, RHEL, CentOS, Amazon Linux).
- **wapiti**: allows to audit the security of web applications. It performs "black-box" scans, i.e. it does not study the source code of the application but will scan the web pages of the deployed web applications, looking for scripts and forms where it can inject data. Once it gets this list, Wapiti acts like a fuzzer, injecting

payloads to see if a script is vulnerable. In this case is necessary to install a scripted/complex web page sites in order to test this package (i.e. https://www.free-css.com/free-css-templates)

- **Kali distribution (https://www.kali.org/)**: There are various other scanners available free and inbuilt in Kali Linux OS.
- Other tools: Tools and software that are used in mobiles as scanners include the names such as Umit Network Scanner, Fing, IP network Scanner, PortDroid network Analysis, Panm IP Scanner, Nessus Vulnerability Scanner, Shadow Sec Scanner, etc.

Contramesures against scanner:

- Configure firewalls (**iptables**) and IDS (**snort**) to detect and block probes.
- Use custom rules to lock down the network and block unwanted ports.
- Run port Scanning tools to determine whether the firewall accurately detects the port scanning activities.
- Security Experts should ensure the proper configuration of anti-scanners and anti-spoofing rules.
- Security experts of an organization must also ensure that the IDS, routers, and firewall firmware are updated to their latest releases.

References: Ethical Hacking, Cibersecurity, TutorialsPoint, MygreatLearning, Coursera, Portal-Offensive.