Application Penetration Testing

Aim:

To familiarize Application Penetration Testing for Network Foot printing (Reconnaissance) and Vulnerability Assessment

Description:

Network Footprinting is the process of identifying and understanding the security risks present in an organization. Like reconnaissance, it involves gathering as much information about the target as possible, including information that may not be readily available online. This information can then be used to build a profile of the organization's security posture and identify potential vulnerabilities.

There are two main types of footprinting: passive and active.

- Passive footprinting: Gathering information from publicly available sources such as websites, news articles, and company profiles
- Active footprinting: Using more intrusive methods to access sensitive data, such as hacking into systems or applying social engineering techniques

The type of footprinting approach you use will depend on what information you want to collect and how much access you have to the target. For example, if you're going to collect information about an organization's network infrastructure, you may need to use active footprinting methods such as port scanning and vulnerability assessment. However, passive footprinting will suffice if you want to gather publicly available information, such as the names of employees and their contact details.

Footprinting is a part of a larger process known as reconnaissance. Reconnaissance is the information-gathering stage of ethical hacking, where you collect data about the target system. This data can include anything from network infrastructure to employee contact details. The goal of reconnaissance is to identify as many potential attack vectors as possible.

Data collected from reconnaissance may include:

- Security policies. Knowing an organization's security policies can help you find weaknesses in their system.
- Network infrastructure. A hacker needs to know what type of network the target is using (e.g., LAN, WAN, MAN), as well as the IP address range and subnet mask.

- Employee contact details. Email addresses, phone numbers, and social media accounts can be used to launch social engineering attacks.
- Host information. Information about specific hosts, such as operating system type and version, can be used to find vulnerabilities.

There are many different ways to approach footprinting, but all approaches should follow a similar methodology. This includes identifying the assessment goals, gathering information about the target, analyzing this information, and reporting your findings.

The information gathered during a footprinting assessment can be used in many different ways. It can be used to improve an organization's security posture by identifying vulnerabilities and recommending corrective actions. Finally, it can also be used as evidence in the aftermath of a data breach or cyberattack. Having a comprehensive record of its security posture can help an organization show that it took all reasonable steps to protect its data. Footprinting in ethical hacking is a common technique used by security professionals to assess an organization's security posture. It can be used as part of a more extensive assessment or in isolation and can provide valuable information about the organization's cybersecurity vulnerabilities.

For hackers, footprinting can be used to gather information about a target that can then be incorporated when planning an attack. This includes information such as the names of employees, contact details, and social media profiles.

Procedure:

Maltego

Maltego is an open-source intelligence forensic application. Which will help you to get more accurate information and in a smarter way. In simple words, it is an information-gathering tool.

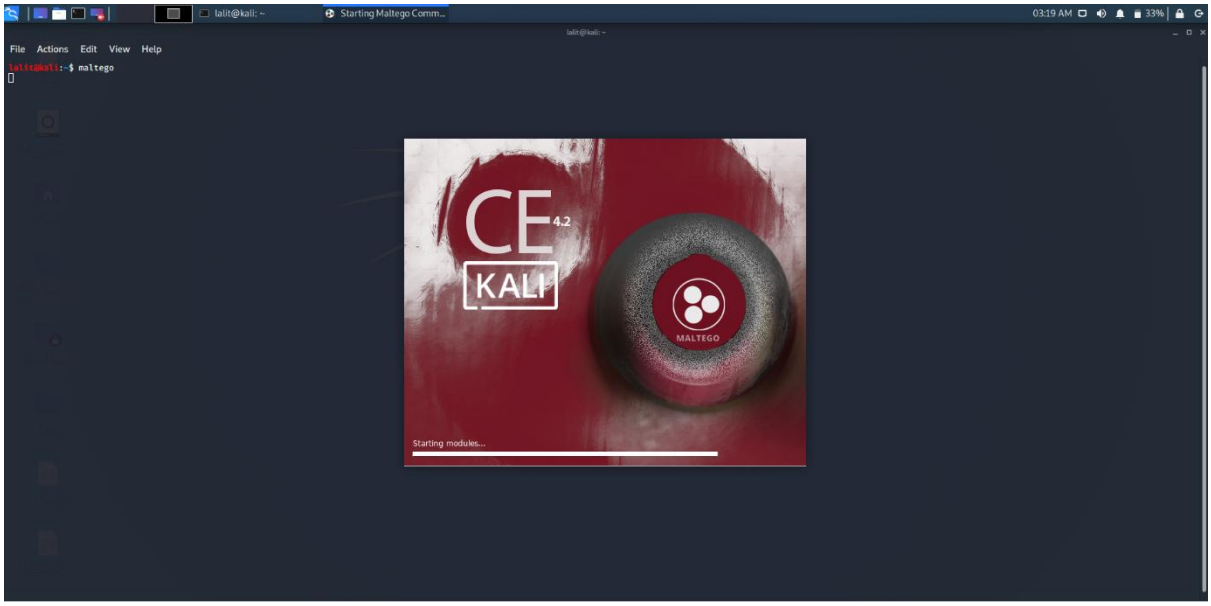
Features of Maltego:

- It is used for gathering information for security related work. It will save your time and make you work smarter and accurately.
- It will help you in the thinking process by demonstrating connected links between all the searched items.
- If you want to get hidden information, it(Maltego) can help you to discover it.

Using Maltego tool in Kali Linux

1. Open Terminal and type “maltego” to run Maltego tool:

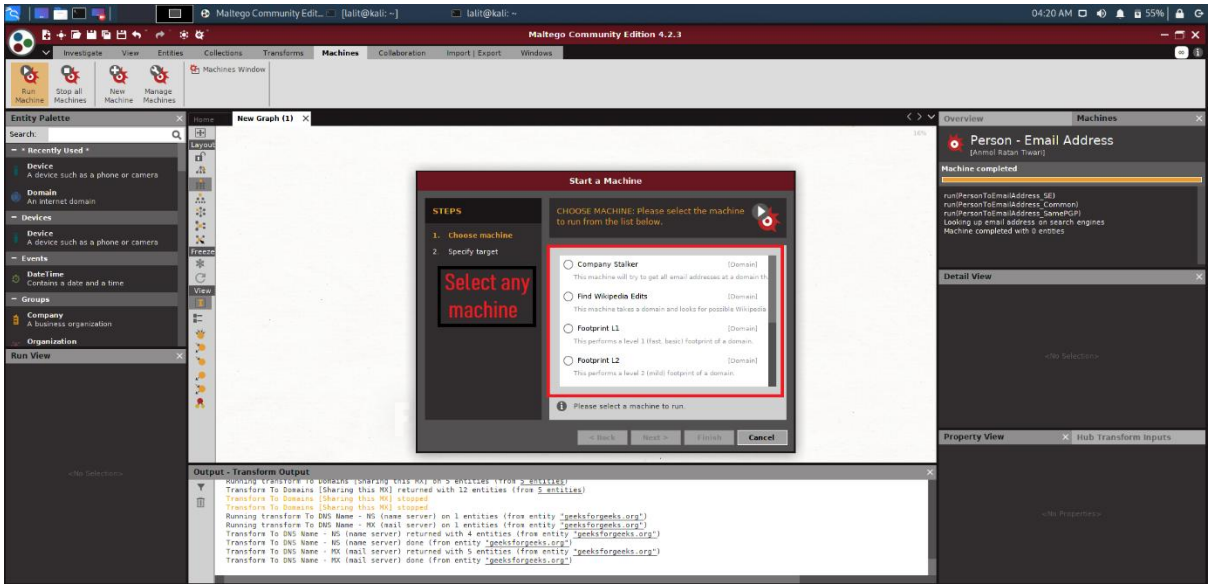
maltego



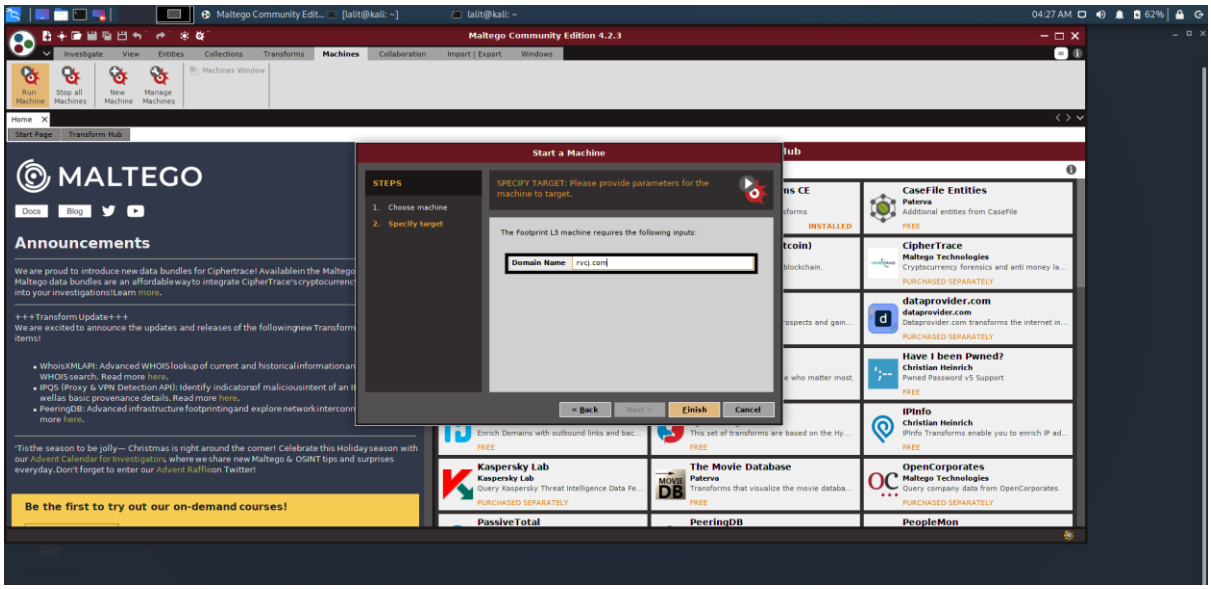
2.First register to use Maltego and remember the password for the next time login into Maltego. After the registration process, log in to Maltego.

3. After that click on **Machines** and then choose **Run Machine.**

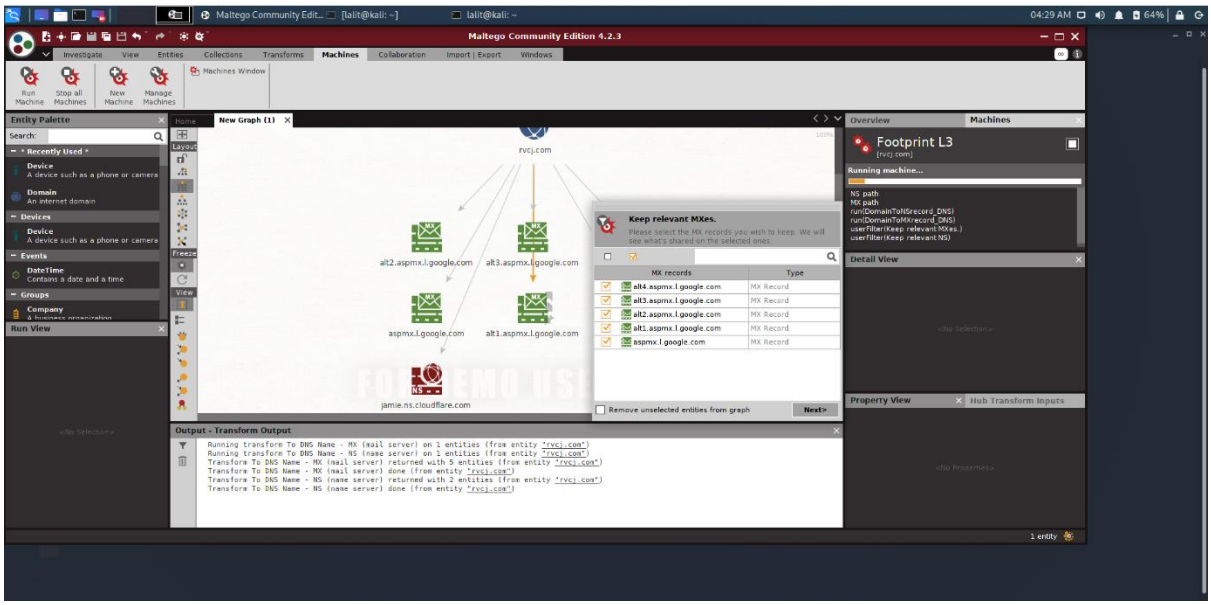
Machine: A machine is simply what type of foot printing we want to do against our target. Select the machine that you want to use.



4. Once choosing a machine for our footprinting. Then choose a Target.



5. Maltego will now begin to gather info on our target and display it on screen as below:



Using Nmap for Local Networks

Running an Nmap scan is often the best way to discover the size of the network and the number of devices that are connected to it. Running a "fast" Nmap scan (**-F**) on a network range can produce a list of all of the IP addresses belonging to active hosts on the network, plus some extra information.

```
sudo nmap -F 192.168.0.0/24

Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-10 22:55 PST
Nmap scan report for 192.168.0.1
Host is up (0.048s latency).
Not shown: 96 closed ports
PORT     STATE    SERVICE
80/tcp   open     http
443/tcp  open     https
5000/tcp open     upnp
8081/tcp filtered blackice-icecap
MAC Address: AC:EC:80:00:EA:17 (Arris Group)

Nmap scan report for 192.168.0.35
Host is up (0.065s latency).
Not shown: 93 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
23/tcp   open  telnet
80/tcp   open  http
443/tcp  open  https
515/tcp  open  printer
631/tcp  open  ipp
9100/tcp open  jetdirect
MAC Address: C4:8E:8F:38:61:93 (Hon Hai Precision Ind.)

Nmap scan report for 192.168.0.232
Host is up (0.032s latency).
All 100 scanned ports on 192.168.0.232 are closed
MAC Address: 60:A3:7D:30:24:60 (Apple)
```

The data provided, combined with some basic information about services a device is running, can be used by itself as a list of targets for other hacking tools, but the capabilities of Nmap go far beyond simple host discovery.

The amount of info on a local network an Nmap scan can gather is impressive, including the MAC address and manufacturer of connected devices, the operating system a device is using, and the version of any services that are running on the device.

Another key function of Nmap is to allow for port scanning of either individual devices or ranges of IP addresses including many devices. This allows an attacker to learn the minute details of a device they have discovered on a network, including information about ports open and services running. Ports are gateways that another device can connect through, so finding

a bunch of services running on open ports can be a huge benefit to a hacker, especially if one of them has a version that is out of date and vulnerable.

Using Nmap for Remote Networks

In addition to scanning local networks, Nmap can also show information about remote networks as well.

```
nmap -F wonderhowto.com

Starting Nmap 7.60 ( https://nmap.org ) at 2018-11-11 23:20 PST
Nmap scan report for wonderhowto.com (104.193.19.59)
Host is up (0.14s latency).
Not shown: 95 closed ports
PORT    STATE    SERVICE
53/tcp  filtered domain
80/tcp  open     http
139/tcp filtered netbios-ssn
443/tcp open     https
445/tcp filtered microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 3.21 seconds
```

After grabbing the IP address and taking note of the port numbers that are open, further Nmap scans can reveal the operating system (**-O**) being used to host a remote website.

```
sudo nmap -O 104.193.19.59

Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-10 23:00 PST
Nmap scan report for wonderhowto.com (104.193.19.59)
Host is up (0.036s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https
Device type: load balancer
Running (JUST GUESSING): Citrix embedded (95%)
Aggressive OS guesses: Citrix NetScaler load balancer (95%), Citrix NetScaler VPX
load balancer (88%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 17 hops

OS detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.69 seconds
```

Using the IP address we discovered earlier, run another scan with **-sV** that reveals the versions of software being used on the target machine.

```
sudo nmap -sV 104.193.19.59

Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-10 23:02 PST
Nmap scan report for wonderhowto.com (104.193.19.59)
Host is up (0.053s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE  VERSION
80/tcp  open  http     Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
443/tcp open  ssl/http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 29.27 seconds
```

These details combined — the IP address of a remote website or server, the operating system running on the device, and the version of any application running on open ports we discover — is everything a hacker needs to get started attacking devices on a network.

Result

Familiarized application penetration testing for network footprinting & vulnerability assessment.