**Experiment No. 7**

# Title: Passive Recon Tools

**Roll No.: 16010420075 Experiments No.: 7**

# Aim: Exploring Passive Recon Tools

\

**Resources:** virtual box

**Theory**

Passive reconnaissance entails examining publicly available information in general. This information is typically gathered from multiple web sources or directly from personnel of the targeted firm. The pentester or attacker does not interact directly with the target machine during this process. There are no logs or traces of the attacker's activities. At first, passive reconnaissance is conducted in order to avoid making physical contact with the target, which could signal an impending assault or betray the attacker's identity.

For example, an attacker could gain access to a target company's business website, read many pages, download documents for additional inquiry, and so forth. These contacts are often overlooked as a precursor to a targeted attack since they are considered typical.

Other more relevant sources of intelligence collection can be included in passive reconnaissance. Here are a few of the most popular methods:

* OSINT stands for open-source intelligence.
* [IPv4 and IPv6] DNS reconnaissance and route mapping
* User data is being gathered.
* Creating a password profile for a user.

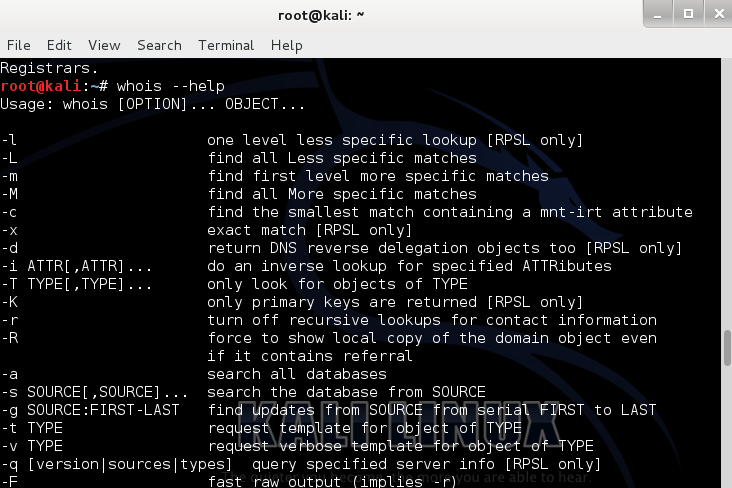
**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**IMPLEMENTATION AND RESULTS:**

Some recon tools are:

1. WHOIS

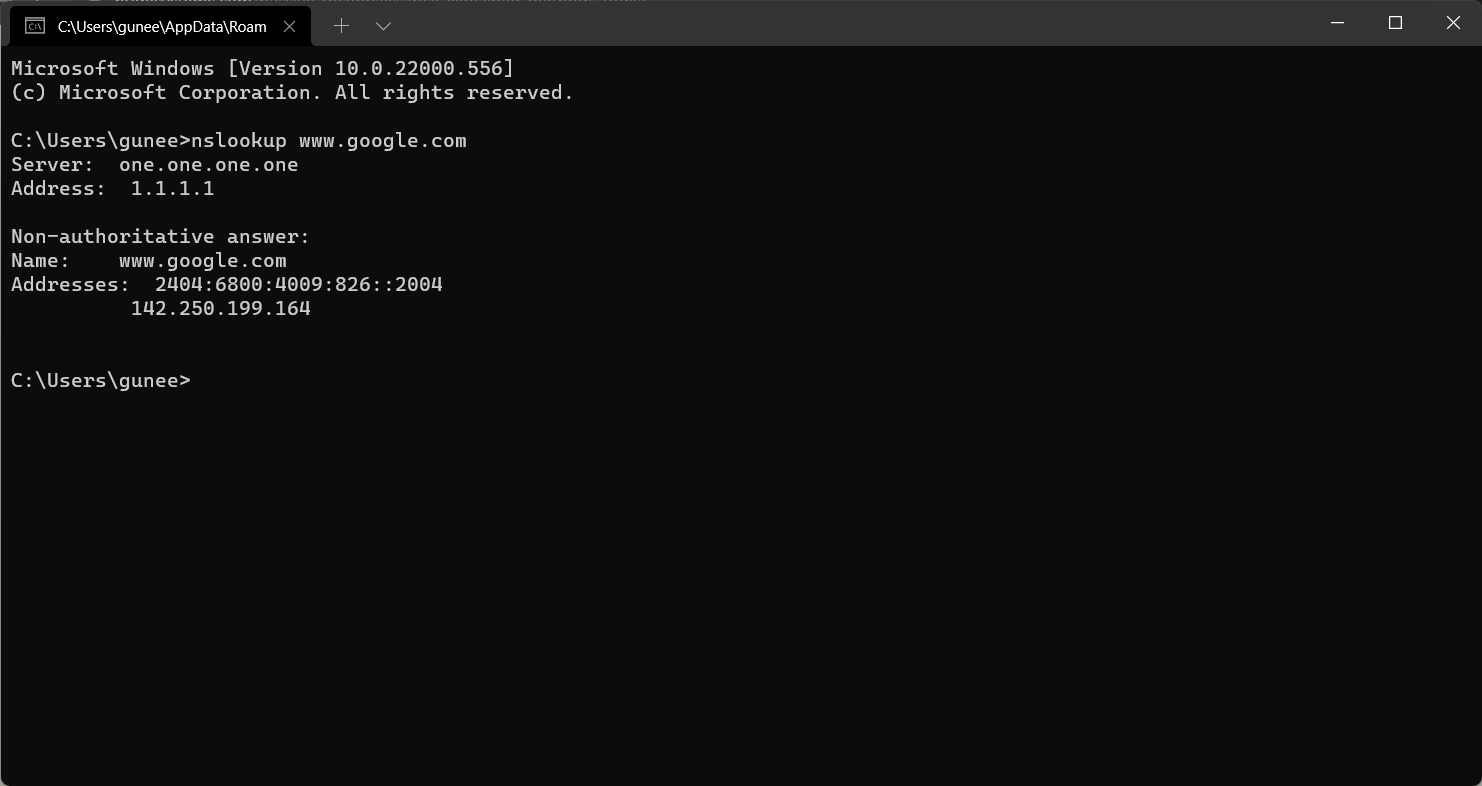
The most convenient approach to execute a whois query on a target is to use the whois target IP or domain name> command from a command prompt, as shown in the image.



The most convenient approach to execute a whois query on a target is to use the whois target IP or domain name> command from a command prompt, as shown in above image.

1. DNS Lookup

On Windows and Linux/UNIX, essential command tools for DNS lookup, such as nslookup, are available. A command-line utility named dig is available on Linux/UNIX computers.



Unfortunately, only one machine can be queried at a time using the nslookup and dig commands. Kali Linux includes a number of tools for iteratively requesting DNS information for IPv4 and IPv6 addresses for a given target.

1. theHarvester

TheHarvester utility is a Python software that uses major search engines to scan for email addresses, servers, and subdomains. TheHarvester is simple to use, as it just requires a few command-line switches to get it up and running.



1. Mapping route to target

Route mapping was created as a diagnostic tool for tracing an IP packet's path from one host to the next.

Each hop from one point to the next, using the Time to Live (TTL) field in an IP packet, leads the receiving router to deliver an ICMP TIME EXCEEDED message, lowering the TTL field value by one.



1. Nmap

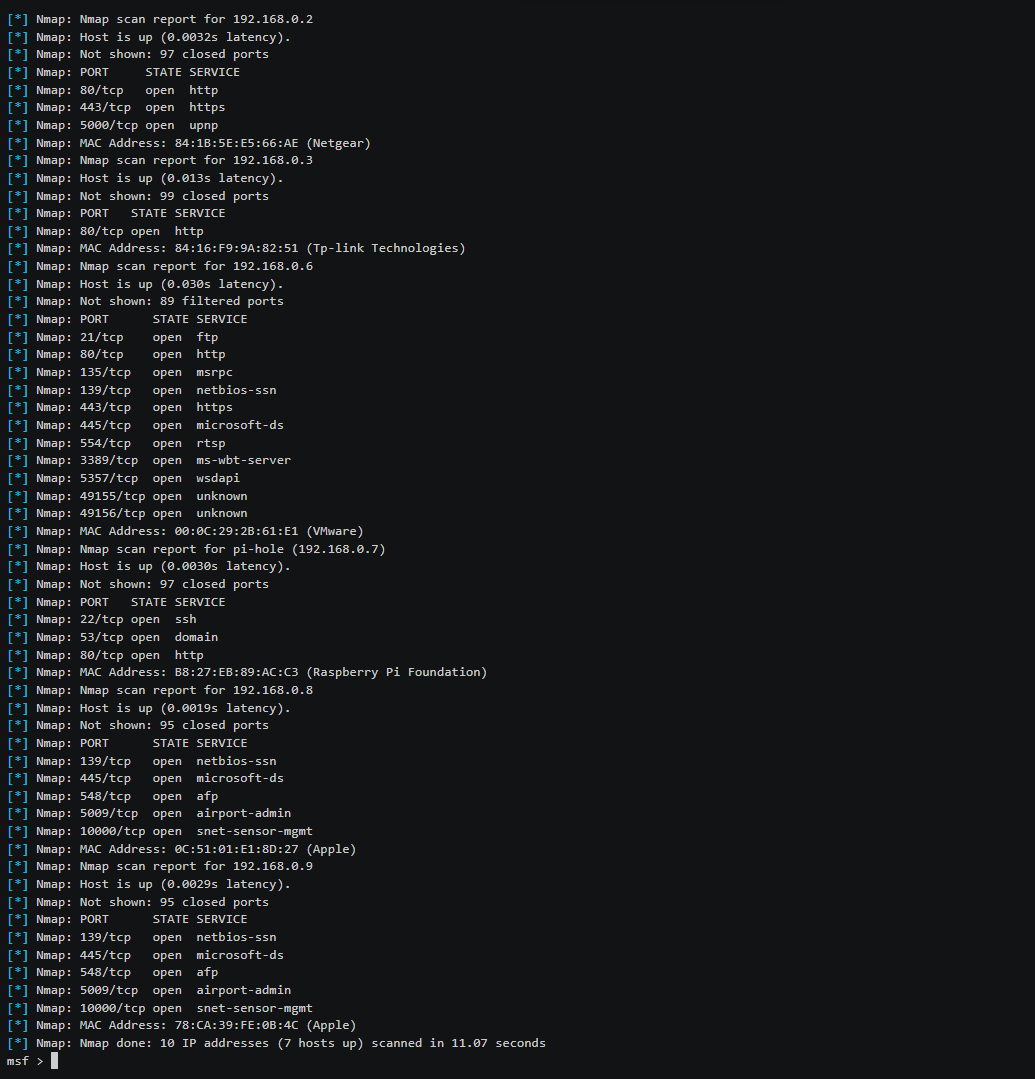
The most well-known tool for active network reconnaissance is Nmap. Nmap is a network scanner that may be used to find out information about a system and the programs that execute on it. This is accomplished by employing a variety of scan types that take use of the specifics of how a system or service works. A hacker can learn a lot about a target network by running scans against a system or a range of IP addresses that are under the target's control.



1. Metasploit

Metasploit was created with the intention of being used as an exploitation toolkit. It includes a number of modules with pre-packaged exploits for a variety of vulnerabilities. Even a rookie hacker can use Metasploit to gain access to a wide range of susceptible machines.

Metasploit, despite being built as an exploit toolkit, can also be used for reconnaissance. At the very least, employing Metasploit's autopwn option allows a hacker to try whatever method possible to exploit a victim. A hacker can use Metasploit to undertake reconnaissance with more subtlety if they conduct more targeted analysis.

****

**Outcomes:**

**CO-1:** Realize that premise of vulnerability analysis and penetration

testing (VAPT).

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Conclusion: (Conclusion to be based on the objectives and outcomes achieved)**

Passive recon tools were listed.

**Grade: AA / AB / BB / BC / CC / CD /DD**

**Signature of faculty in-charge with date**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**REFERENCES:**

* [www.kali.org](http://www.kali.org)