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:

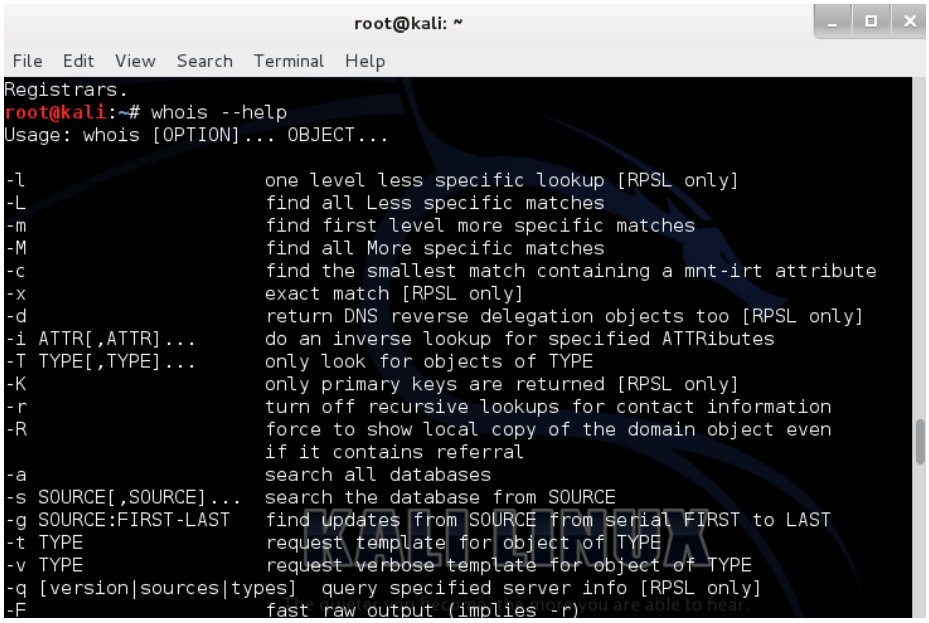
- OSINT stands for open-source intelligence.
- [IPv4 and IPv6] DNS reconnaissance and route mapping
- User data is being gathered.
- Creating a password profile for a user.

IMPLEMENTATION AND RESULTS:

Some recon tools are:

1. WHOIS

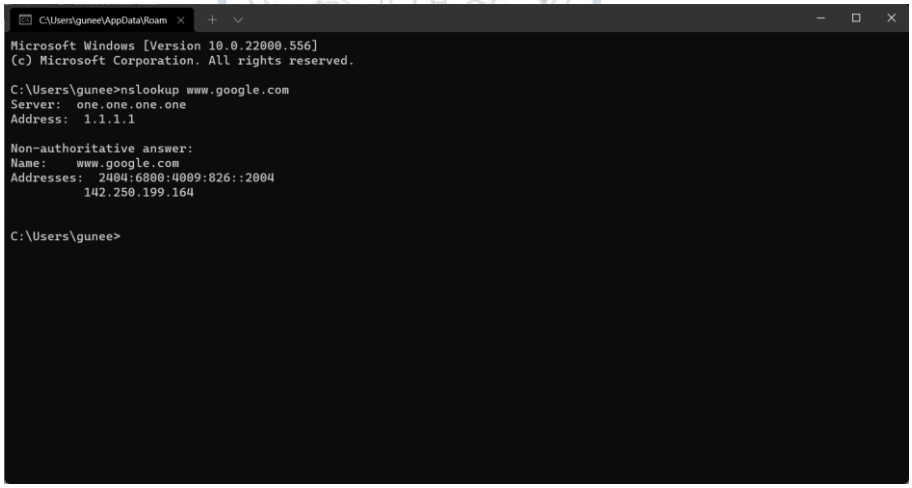
   The most convenient approach to execute a whois query on a target is to use the whois target IP or domain name> command from a command prompt, as shown in the image.



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.

2. 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.

3. 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.

```
root@kali:~# theharvester -b all -d zonetransfer.me

*******************************************************************
*                                                                 *
* | |_| |__   ___    /\  /\__ _ _ ____   _____  ___| |_ ___ _ __ *
* | __| '_ \ / _ \  / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|    *
*                                                                 *
* TheHarvester Ver. 2.7                                           *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*******************************************************************


Full harvest..
[-] Searching in Google..
        Searching 0 results...
        Searching 100 results...
[-] Searching in PGP Key server..
[-] Searching in Bing..
        Searching 50 results...
        Searching 100 results...
[-] Searching in Exalead..
        Searching 50 results...
        Searching 100 results...
        Searching 150 results...


[+] Emails found:
------------------
pippa@zonetransfer.me
pixel-1506786993611511-web-@zonetransfer.me
pixel-1506786996891728-web-@zonetransfer.me
xss.zonetransfer.me@xss.zonetransfer.me

[+] Hosts found in search engines:
------------------------------------
[-] Resolving hostnames IPs...
127.0.0.1:asfdbbox.zonetransfer.me
4.23.39.254:office.zonetransfer.me
207.46.197.32:owa.zonetransfer.me
54.206.51.177:staging.zonetransfer.me
217.147.177.157:testing.zonetransfer.me
217.147.177.157:www.zonetransfer.me
[+] Virtual hosts:
```

4. 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.

```
C:\Users\gunee>tracert www.google.com

Tracing route to www.google.com [142.250.76.164]
over a maximum of 30 hops:

  1     5 ms     1 ms    36 ms  192.168.0.1
  2     3 ms     2 ms     2 ms  175.100.185.144
  3     3 ms     *        5 ms  175.100.180.129
  4   105 ms     7 ms    18 ms  172.16.2.202
  5     8 ms     7 ms    10 ms  175.100.188.22
  6     5 ms     5 ms     5 ms  142.251.225.29
  7     6 ms    11 ms     4 ms  216.239.46.137
  8     3 ms     3 ms     3 ms  bom12s09-in-f4.1e100.net [142.250.76.164]

Trace complete.
```

5. 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.

```
root@kali:~# nmap 192.168.56.102

Starting Nmap 6.47 ( http://nmap.org ) at 2015-06-09 21:15 CDT
Nmap scan report for 192.168.56.102
Host is up (0.00041s latency).
Not shown: 991 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
139/tcp  open  netbios-ssn
143/tcp  open  imap
443/tcp  open  https
445/tcp  open  microsoft-ds
5001/tcp open  commplex-link
8080/tcp open  http-proxy
8081/tcp open  blackice-icecap
MAC Address: 08:00:27:3F:C5:C4 (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 0.30 seconds
```

6. 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.

```
[*] Nmap: Nmap scan report for 192.168.0.2
[*] Nmap: Host is up (0.0032s latency).
[*] Nmap: Not shown: 97 closed ports
[*] Nmap: PORT     STATE SERVICE
[*] Nmap: 80/tcp   open  http
[*] Nmap: 443/tcp  open  https
[*] Nmap: 5000/tcp open  upnp
[*] Nmap: MAC Address: 84:1B:5E:E5:66:AE (Netgear)
[*] Nmap: Nmap scan report for 192.168.0.3
[*] Nmap: Host is up (0.013s latency).
[*] Nmap: Not shown: 99 closed ports
[*] Nmap: PORT   STATE SERVICE
[*] Nmap: 80/tcp open  http
[*] Nmap: MAC Address: 84:16:F9:9A:82:51 (Tp-link Technologies)
[*] Nmap: Nmap scan report for 192.168.0.6
[*] Nmap: Host is up (0.030s latency).
[*] Nmap: Not shown: 89 filtered ports
[*] Nmap: PORT      STATE SERVICE
[*] Nmap: 21/tcp    open  ftp
[*] Nmap: 80/tcp    open  http
[*] Nmap: 135/tcp   open  msrpc
[*] Nmap: 139/tcp   open  netbios-ssn
[*] Nmap: 443/tcp   open  https
[*] Nmap: 445/tcp   open  microsoft-ds
[*] Nmap: 554/tcp   open  rtsp
[*] Nmap: 3389/tcp  open  ms-wbt-server
[*] Nmap: 5357/tcp  open  wsdapi
[*] Nmap: 49155/tcp open  unknown
[*] Nmap: 49156/tcp open  unknown
[*] Nmap: MAC Address: 00:0C:29:2B:61:E1 (VMware)
[*] Nmap: Nmap scan report for pi-hole (192.168.0.7)
[*] Nmap: Host is up (0.0030s latency).
[*] Nmap: Not shown: 97 closed ports
[*] Nmap: PORT   STATE SERVICE
[*] Nmap: 22/tcp open  ssh
[*] Nmap: 53/tcp open  domain
[*] Nmap: 80/tcp open  http
[*] Nmap: MAC Address: B8:27:EB:89:AC:C3 (Raspberry Pi Foundation)
[*] Nmap: Nmap scan report for 192.168.0.8
[*] Nmap: Host is up (0.0019s latency).
[*] Nmap: Not shown: 95 closed ports
[*] Nmap: PORT      STATE SERVICE
[*] Nmap: 139/tcp   open  netbios-ssn
[*] Nmap: 445/tcp   open  microsoft-ds
[*] Nmap: 548/tcp   open  afp
[*] Nmap: 5009/tcp  open  airport-admin
[*] Nmap: 10000/tcp open  snet-sensor-mgmt
[*] Nmap: MAC Address: 0C:51:01:E1:8D:27 (Apple)
[*] Nmap: Nmap scan report for 192.168.0.9
[*] Nmap: Host is up (0.0029s latency).
[*] Nmap: Not shown: 95 closed ports
[*] Nmap: PORT      STATE SERVICE
[*] Nmap: 139/tcp   open  netbios-ssn
[*] Nmap: 445/tcp   open  microsoft-ds
[*] Nmap: 548/tcp   open  afp
[*] Nmap: 5009/tcp  open  airport-admin
[*] Nmap: 10000/tcp open  snet-sensor-mgmt
[*] Nmap: MAC Address: 78:CA:39:FE:0B:4C (Apple)
[*] Nmap: Nmap done: 10 IP addresses (7 hosts up) scanned in 11.07 seconds
msf >
```

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