Reconnaissance – Part II

Tools in Kali Linux

Module #16

Reconnaissance : Tools - HTTrack

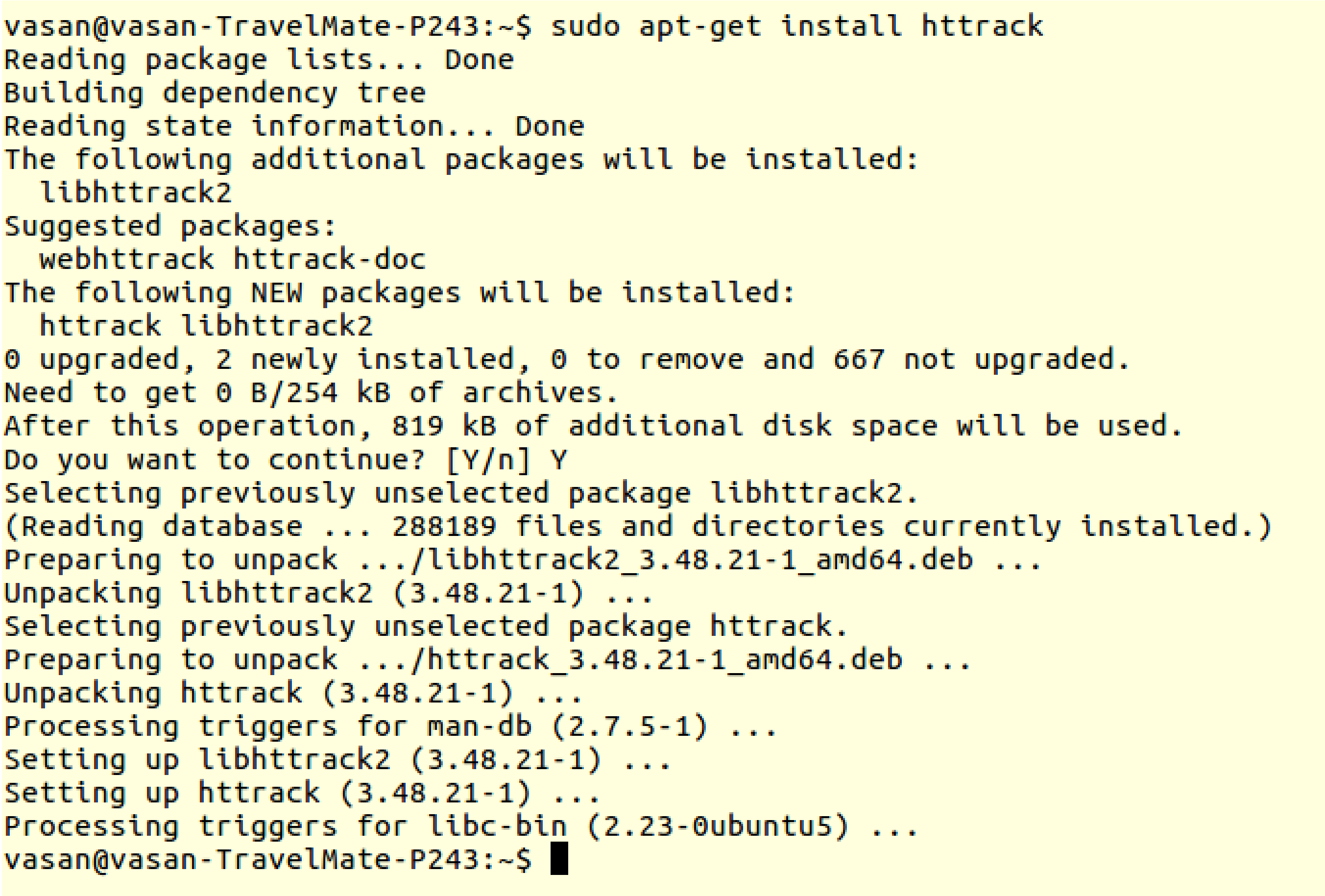
HTTrack is a tool built into Kali Linux.

The purpose of HTTrack is to copy a website.

Helps one to look at the entire content of a website, all its pages, and files offline, and in their own controlled environment.

In addition, we can use HTTrack for social engineering attacks. Having a copy of a website could be used to develop fake phishing websites, which can be incorporated in other Penetration Testing toolsets.

Reconnaissance : Tools - HTTrack



```
vasan@vasan-TravelMate-P243:~$ sudo apt-get install httrack
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libhttrack2
Suggested packages:
  webhttrack httrack-doc
The following NEW packages will be installed:
  httrack libhttrack2
0 upgraded, 2 newly installed, 0 to remove and 667 not upgraded.
Need to get 0 B/254 kB of archives.
After this operation, 819 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Selecting previously unselected package libhttrack2.
(Reading database ... 288189 files and directories currently installed.)
Preparing to unpack .../libhttrack2_3.48.21-1_amd64.deb ...
Unpacking libhttrack2 (3.48.21-1) ...
Selecting previously unselected package httrack.
Preparing to unpack .../httrack_3.48.21-1_amd64.deb ...
Unpacking httrack (3.48.21-1) ...
Processing triggers for man-db (2.7.5-1) ...
Setting up libhttrack2 (3.48.21-1) ...
Setting up httrack (3.48.21-1) ...
Processing triggers for libc-bin (2.23-0ubuntu5) ...
vasan@vasan-TravelMate-P243:~$ █
```

ICMP Reconnaissance

Recall: ICMP is a protocol used for network troubleshooting.
Two most popular applications using ICMP: Ping and traceroute
These tools are installed by default currently in all Oses

Penetration testing with these tools:

- Most high security conscious systems will have the ICMP protocol disabled
- Excessive usage of these tools will trigger alerts for the administrator of a possible impending attack
- If there are responses received from for the tool, we can infer that the target is alive
- If there is a timeout, either the ICMP is blocked or the target is currently down

DNS Reconnaissance

Recall: DNS is a protocol used for converting a host name to an IP Address

DNS gives the necessary information to the Penetration tester for mapping the system and subdomain

DNS by nature responds to queries – An attacker could use a query with a list of words to the DNS server to get the list of IP Addresses.

This is however extremely time consuming task that can also be automated.

Dig (Domain Information Groper)

Dig is the most popularly used DNS reconnaissance tool. Using Dig, a specific DNS server can be queried directly

DNS gives the necessary information to the Penetration tester for mapping the system and subdomain

DNS by nature responds to queries – An attacker could use a query with a list of words to the DNS server to get the list of IP Addresses.

This is however extremely time consuming task that can also be automated.

DNS Reconnaissance in Kali Linux

“Information Gathering” → “DNS Analysis” → Fierce

Reconnaissance : Tools - nmap

Nmap stands for network mapper

Used to scan hosts and services on a network. Nmap has advanced features that can detect different applications running on systems as well as services and OS fingerprinting features.

Kali comes loaded with Zenmap. Zenmap gives Nmap a graphical User interface (GUI) to run commands.

Thank You