National Telecommunication Institute

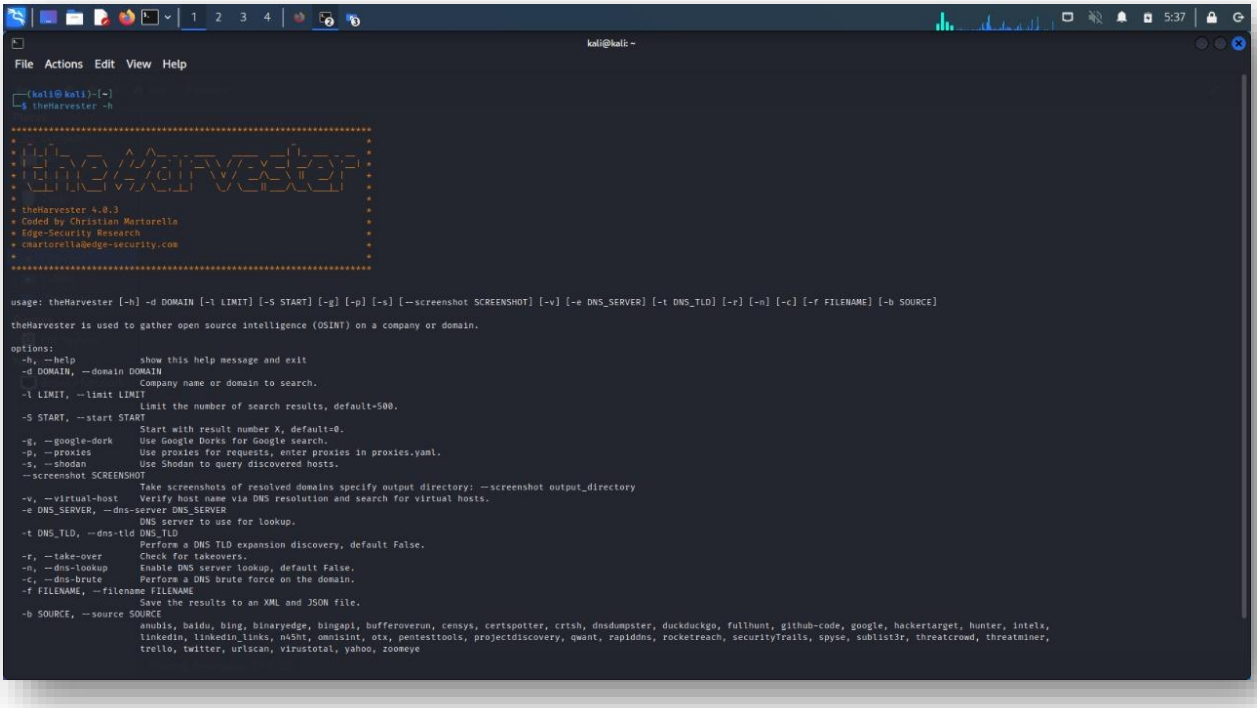
Report about The Harvester tool on Linux

Prepared by: Ahmed Moataz Abdelmonem Elrefaey

- Target Domain Microsoft.com

- The help menu of the Harvester tool

  theHarvester -h

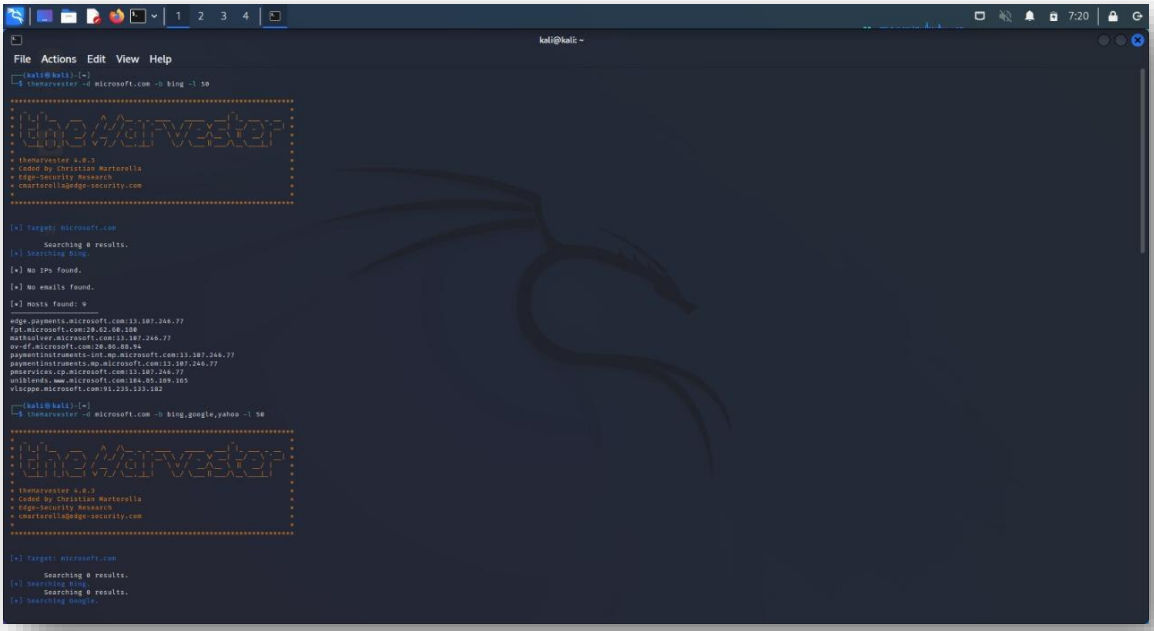


- What types of information did you find?

  I found several subdomains, but I didn't find any emails because most companies remove the important emails for security reasons, but we can find some services emails using search engines like "hunter" using private API.

- subdomains I retrieved with IPs hosting that service.

  theHarvester -d microsoft.com -b bing -l 50



[*] Hosts found: 9

---

edge.payments.microsoft.com:13.107.246.77

fpt.microsoft.com:20.62.60.180

mathsolver.microsoft.com:13.107.246.77

ov-df.microsoft.com:20.86.88.94

paymentinstruments-int.mp.microsoft.com:13.107.246.77

paymentinstruments.mp.microsoft.com:13.107.246.77

pmservices.cp.microsoft.com:13.107.246.77

uniblends.www.microsoft.com:184.85.189.165

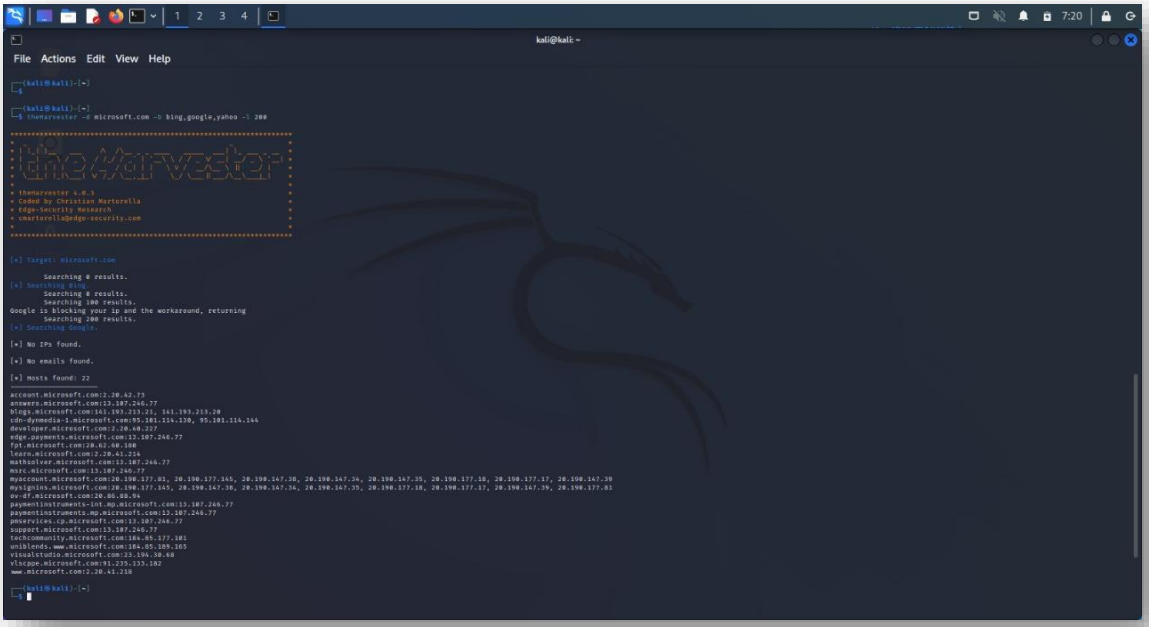
vlscppe.microsoft.com:91.235.133.182

- Which source engine gave the most useful results?

  I found that Bing is useful if I want to search for subdomains but for searching about emails the hunter is the most useful for this.

- How did using multiple sources affect the results?

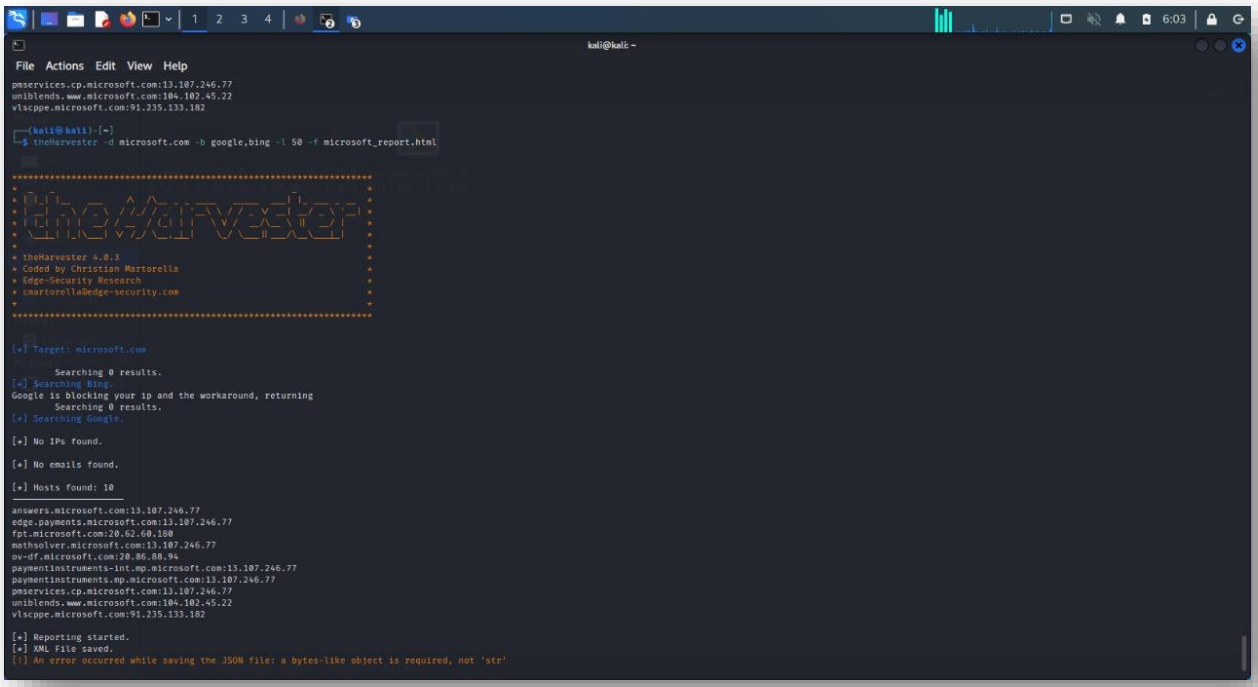
theHarvester -d microsoft.com -b bing,google,yahoo -l 50



[*] Hosts found: 22
---
account.microsoft.com:2.20.42.73
answers.microsoft.com:13.107.246.77
blogs.microsoft.com:141.193.213.21, 141.193.213.20
cdn-dynmedia-1.microsoft.com:95.101.114.130, 95.101.114.144
developer.microsoft.com:2.20.40.227
edge.payments.microsoft.com:13.107.246.77
fpt.microsoft.com:20.62.60.180
learn.microsoft.com:2.20.41.214
mathsolver.microsoft.com:13.107.246.77
msrc.microsoft.com:13.107.246.77
myaccount.microsoft.com:20.190.177.81, 20.190.177.145, 20.190.147.38, 20.190.147.34, 20.190.147.35, 20.190.177.18, 20.190.177.17, 20.190.147.39
mysignins.microsoft.com:20.190.177.145, 20.190.147.38, 20.190.147.34, 20.190.147.35, 20.190.177.18, 20.190.177.17, 20.190.147.39, 20.190.177.81
ov-df.microsoft.com:20.86.88.94
paymentinstruments-int.mp.microsoft.com:13.107.246.77
paymentinstruments.mp.microsoft.com:13.107.246.77
pmservices.cp.microsoft.com:13.107.246.77
support.microsoft.com:13.107.246.77
techcommunity.microsoft.com:184.85.177.101
uniblends.www.microsoft.com:184.85.189.165
visualstudio.microsoft.com:23.194.30.68
vlscppe.microsoft.com:91.235.133.182

- To save output in XML or JSON file

  theHarvester -d microsoft.com -b google,bing -l 200 -f microsoft_report.html



- Are there duplicate entries across engines? How can you filter or clean that?

  Yes, there are duplicate entries across engines, but we can filter or clean it using this command:

  sort results.txt | uniq > clean_results.txt

  “clean_results.txt” this is the file after filtering.

  “results.txt” this file is the file I stored all hosts in (before filtering).

  I stored the output of any command using this command:

  Cat > results.txt

- How much internal data (like employee names or emails) was exposed?

  No important internal data because emails and subdomains which out is services data (public data) but we should focus on the mails comes to these emails because any hacker can use these emails to send phishing mail and hackers can use subdomains and this is the first point to attack using social engineering.

- What did you learn?

  By using theHarvester I learned how OSINT tools can collect information about a target domain from public sources. The tool helped me find some subdomains and see which IP addresses they resolve to. I also noticed that emails are not always easy to find because many search engines block automated queries. Overall, I understood that theHarvester is useful for basic recon, but it has limits and should be combined with other tools like Sublist3r or Amass to get a more complete picture.

- Compare theHarvester results with another tool like Sublist3r or amass. Do they match?

  theHarvester: depends on search engines and some APIs, so it usually finds only a small number of subdomains.
  Sublist3r: a bit better than theHarvester, it can find more subdomains but still limited.
  Amass: the most powerful tool, it can discover hundreds or even thousands of subdomains because it uses many different sources and ASN enumeration.