# Experiment No. 2

**Kaushal Kotkar**

# BE-15

**Roll no: 54**

**Aim:** Using OSINT tool such as (Harvester) you can gather information like emails, subdomains, hosts, employee names, open ports, and banners from different public sources like search engines, PGP key server

**Lab outcome:** Conduct advanced searches to gather intelligence from social media sites and understand the use of Public Records for corporate and business intelligence etc.

# Theory:

TheHarvester is a powerful OSINT (Open-Source Intelligence) tool designed to collect information from various public sources. It allows investigators to gather valuable data related to a target, such as email addresses, subdomains, online profiles, and more. The tool utilizes search engines, social media platforms, and other online resources to compile a comprehensive overview of the digital footprint associated with a specific domain.

# Installation:

In terminal type:

sudo apt-get theHarvester

If it does not work, you can try to clone it directly from git using the following commands git clone <https://github.com/laramies/theHarvester.git>

cd theHarvester

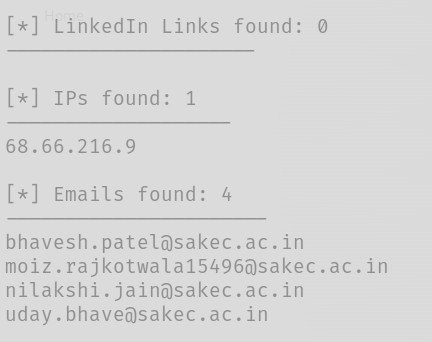
sudo python ./theHarvester.py

# Output

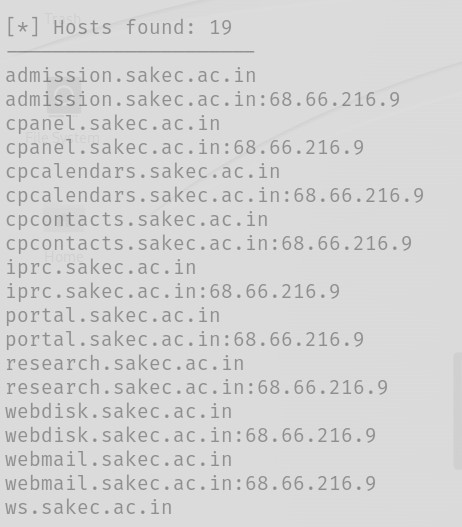
Use theHarvester tool to scan emails, hosts, etc of domain sakec.ac.in



Found IP and emails

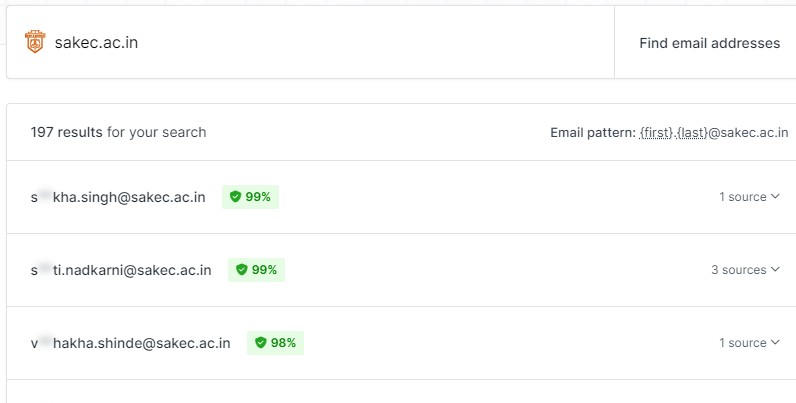


Found hosts



# Hunter

To find email address



# Dnsdumpster

Used for server & asn detection, subdomain & IP





**Conclusion:** By utilizing theHarvester, Dnsdumpster & Hunter we successfully collected a variety of information from diverse sources related to the target domain. The tool's capabilities allowed us to gather email addresses, IP, and other relevant data, providing a comprehensive overview of the digital footprint associated with the domain.