CYBERSECURITY TRAINING

(WEEK 3 – Day2)

Penetration Testing

1.Introduction to Penetration Testing

Definition and Purpose:
Penetration Testing (or Pen Testing) is a simulated cyberattack performed on a computer system, network, or web application to evaluate its security. The main goal is to identify vulnerabilities that malicious hackers could exploit and provide recommendations to fix them. It helps improve an organization's defensive posture before real attacks occur.

2. **Difference Between Vulnerability Assessment and Penetration Testing:**

- **Vulnerability Assessment** is a process of **scanning and identifying known weaknesses** in systems using automated tools.
- **Penetration Testing**, on the other hand, goes a step further to **exploit those vulnerabilities**, simulating a real-world attack to understand the impact and reach of the flaw.
  In short, vulnerability assessment is about **finding**, while pen testing is about **proving** the vulnerability.

3.Types of Penetration Testing:

Black Box Testing:

The tester has **no prior knowledge** of the system. This simulates an **external attack** by an outsider (e.g., a hacker with no internal access). It tests how well the system can be breached without inside help.

White Box Testing:

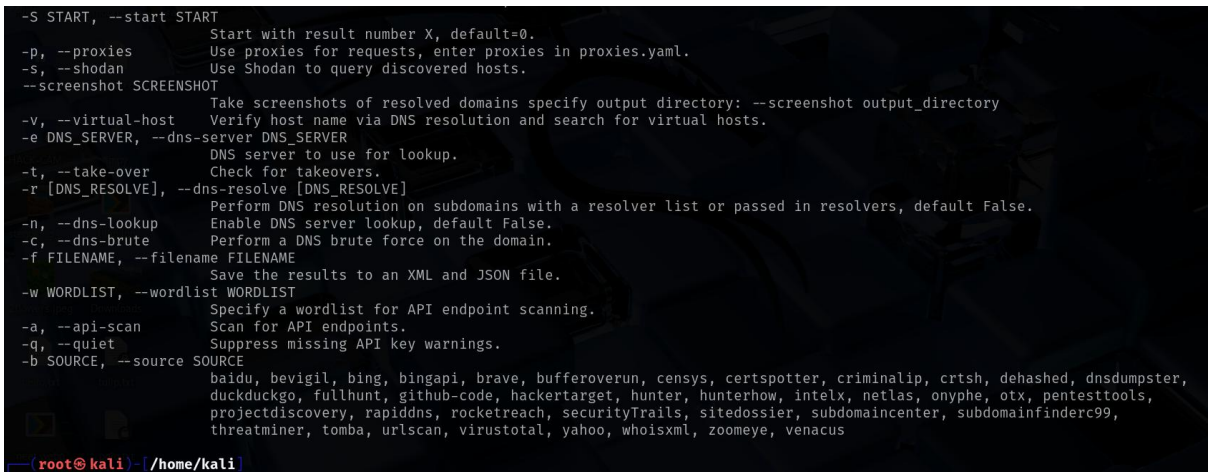
The tester has **full knowledge** of the system including source code, network diagrams, and credentials. This simulates an **insider threat** or trusted employee attack and helps find deeper, complex flaws.

Gray Box Testing:

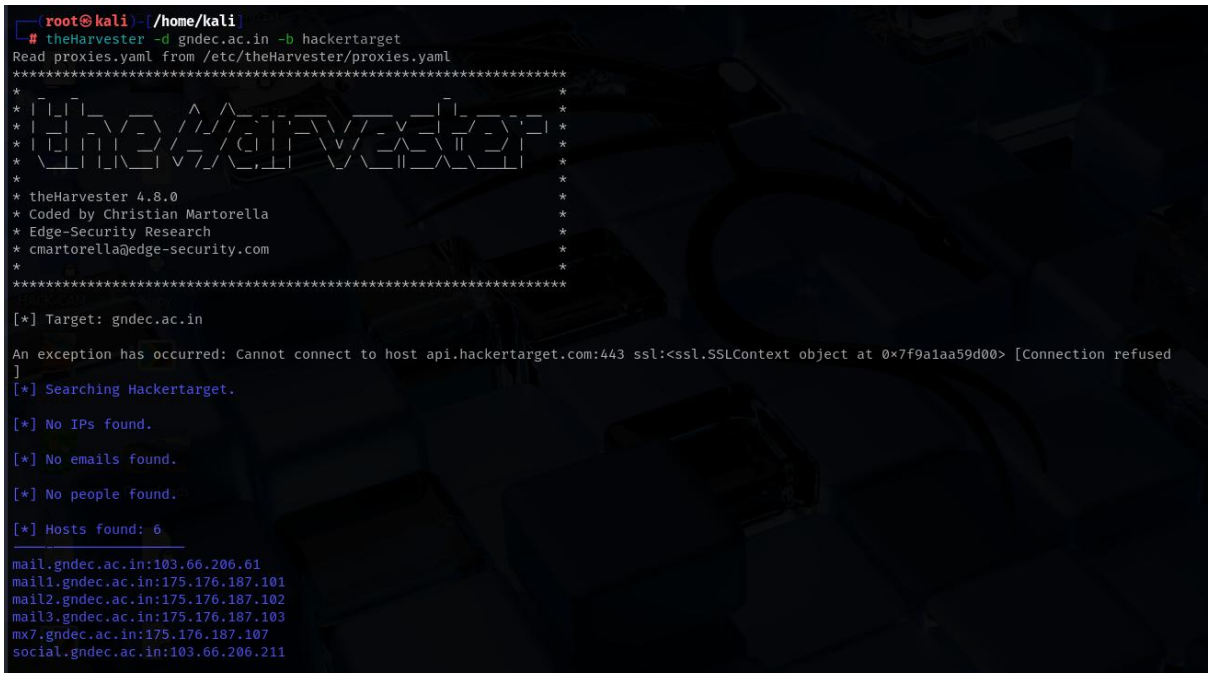
The tester has **partial knowledge** of the system. This simulates an attack from a **semi-privileged user**, such as a contractor or someone with limited access. It balances between Black Box and White Box testing approaches.

Practical Implementation for Information Gathering

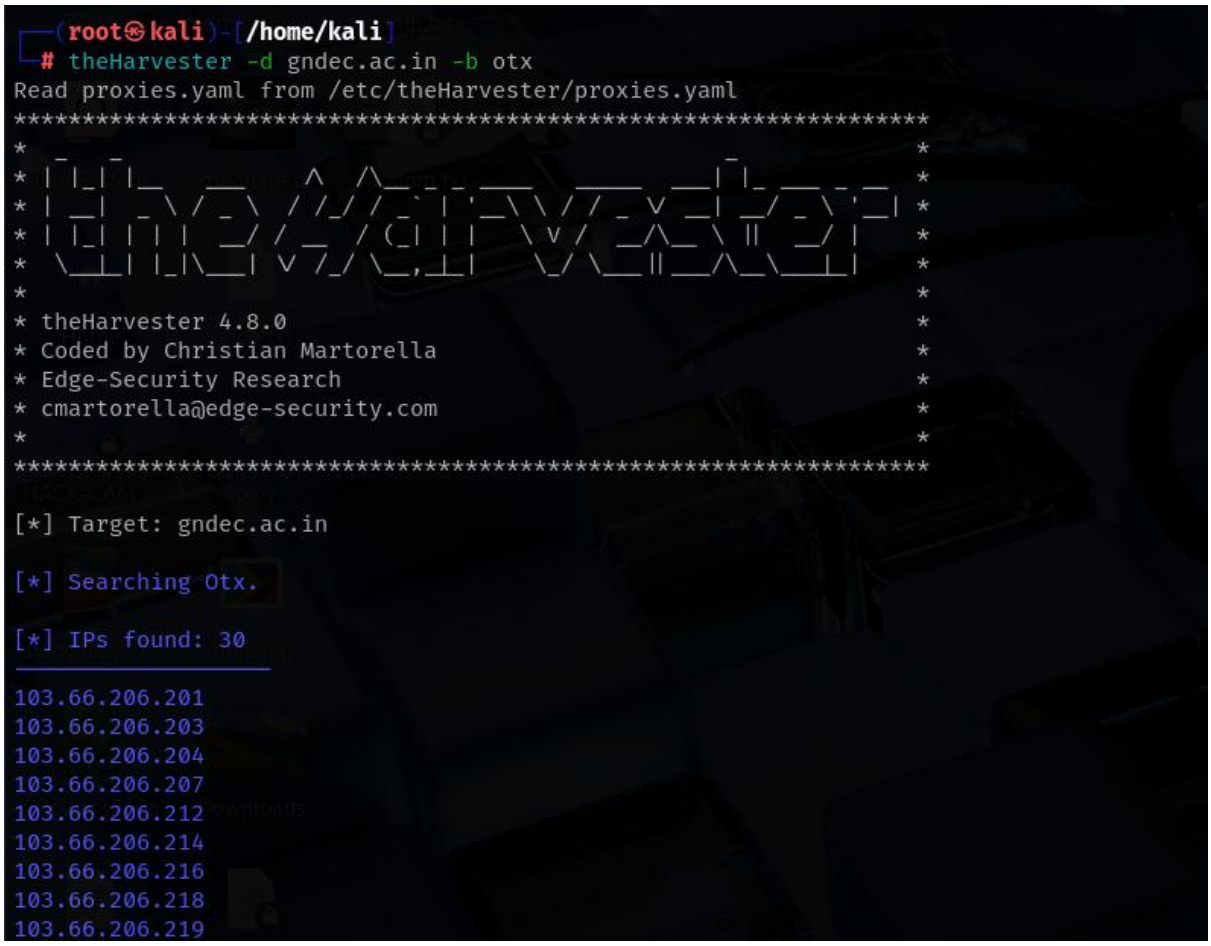
--The tool we are using is: **theHarvesters**

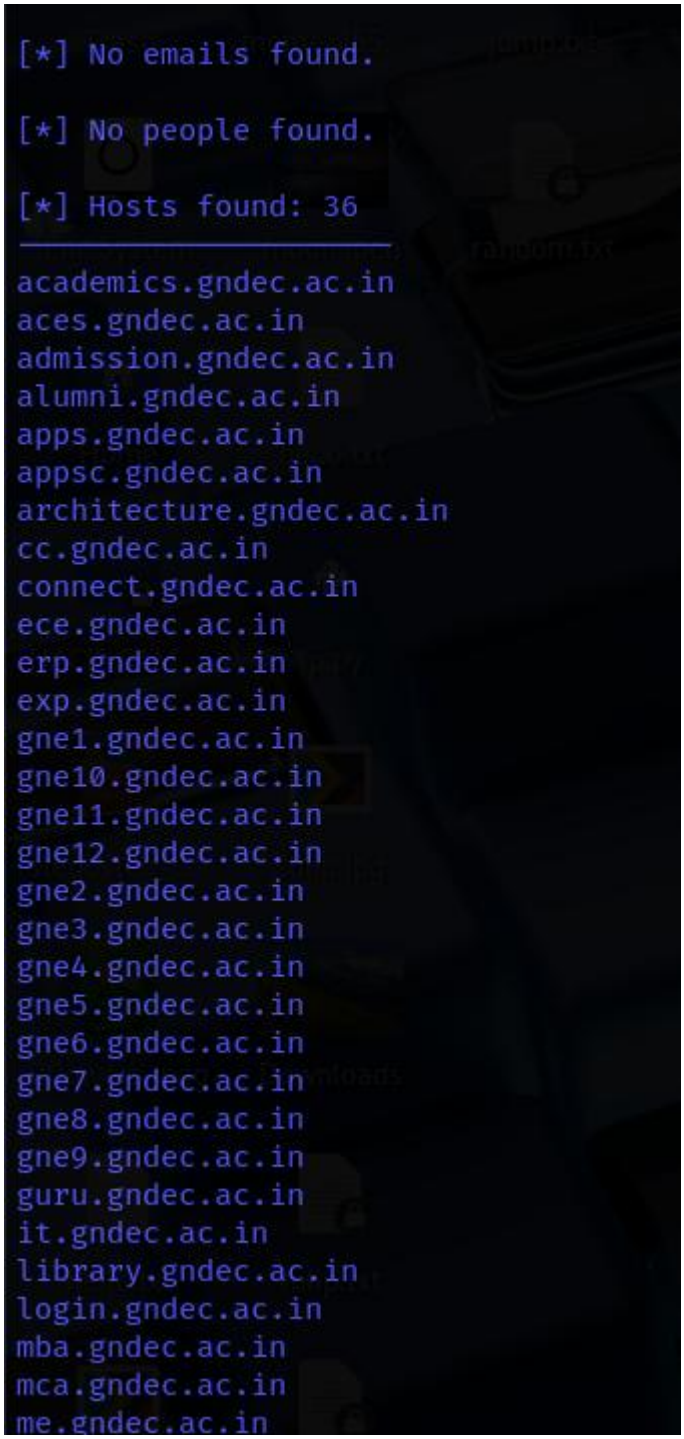


1.Targethacker

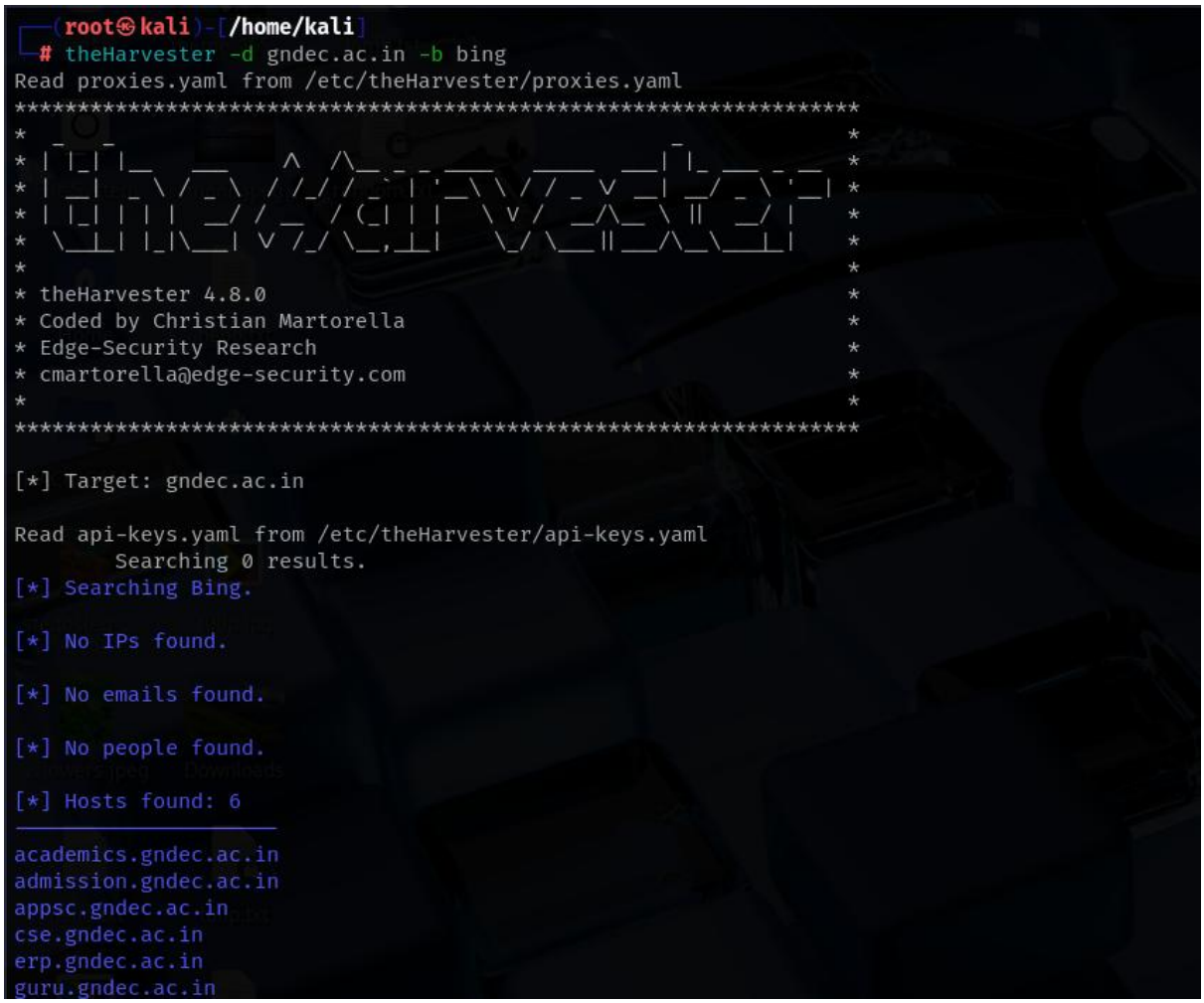


2.OTX




[*] No emails found.
[*] No people found.
[*] Hosts found: 36
academics.gndec.ac.in
aces.gndec.ac.in
admission.gndec.ac.in
alumni.gndec.ac.in
apps.gndec.ac.in
appsc.gndec.ac.in
architecture.gndec.ac.in
cc.gndec.ac.in
connect.gndec.ac.in
ece.gndec.ac.in
erp.gndec.ac.in
exp.gndec.ac.in
gne1.gndec.ac.in
gne10.gndec.ac.in
gne11.gndec.ac.in
gne12.gndec.ac.in
gne2.gndec.ac.in
gne3.gndec.ac.in
gne4.gndec.ac.in
gne5.gndec.ac.in
gne6.gndec.ac.in
gne7.gndec.ac.in
gne8.gndec.ac.in
gne9.gndec.ac.in
guru.gndec.ac.in
it.gndec.ac.in
library.gndec.ac.in
login.gndec.ac.in
mba.gndec.ac.in
mca.gndec.ac.in
me.gndec.ac.in

3.Bing


root kali /home/kali
theHarvester -d gndec.ac.in -b bing
Read proxies.yaml from /etc/theHarvester/proxies.yaml
theHarvester 4.8.0
Coded by Christian Martorella
Edge-Security Research
cmartorella@edge-security.com
[*] Target: gndec.ac.in
Read api-keys.yaml from /etc/theHarvester/api-keys.yaml
Searching 0 results.
[*] Searching Bing.
[*] No IPs found.
[*] No emails found.
[*] No people found.
[*] Hosts found: 6
academics.gndec.ac.in
admission.gndec.ac.in
appsc.gndec.ac.in
cse.gndec.ac.in
erp.gndec.ac.in
guru.gndec.ac.in