

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: **theHarvester**

```
root@kali:~/home/kali# theHarvester -help
Read proxies.yaml from /etc/theHarvester/proxies.yaml
*****
* theHarvester 4.8.0
* Coded by Christian Martorella
* Edge-Security Research
* cmartorella@edge-security.com
*
*****
usage: theHarvester [-h] -d DOMAIN [-l LIMIT] [-S START] [-p] [-s] [--screenshot SCREENSHOT] [-v] [-e DNS_SERVER] [-t] [-r [DNS_RESOLVE]]
                  [-n] [-c] [-f FILENAME] [-w WORDLIST] [-a] [-q] [-b SOURCE]

theHarvester is used to gather open source intelligence (OSINT) on a company or domain.

options:
  -h, --help            show this help message and exit
  -d DOMAIN, --domain DOMAIN
                        Company name or domain to search.
  -l LIMIT, --limit LIMIT
                        Limit the number of search results, default=500.
  -S START, --start START
                        Start with result number X, default=0.
  -p, --proxies          Use proxies for requests, enter proxies in proxies.yaml.
```

```
-S START, --start START
                        Start with result number X, default=0.
-p, --proxies          Use proxies for requests, enter proxies in proxies.yaml.
-s, --shodan           Use Shodan to query discovered hosts.
--screenshot SCREENSHOT
                        Take screenshots of resolved domains specify output directory: --screenshot output_directory
-v, --virtual-host      Verify host name via DNS resolution and search for virtual hosts.
-e DNS_SERVER, --dns-server DNS_SERVER
                        DNS server to use for lookup.
-t, --take-over        Check for takeovers.
-r [DNS_RESOLVE], --dns-resolve [DNS_RESOLVE]
                        Perform DNS resolution on subdomains with a resolver list or passed in resolvers, default False.
-n, --dns-lookup        Enable DNS server lookup, default False.
-c, --dns-brute        Perform a DNS brute force on the domain.
-f FILENAME, --filename FILENAME
                        Save the results to an XML and JSON file.
-w WORDLIST, --wordlist WORDLIST
                        Specify a wordlist for API endpoint scanning.
-a, --api-scan          Scan for API endpoints.
-q, --quiet            Suppress missing API key warnings.
-b SOURCE, --source SOURCE
                        baidu, bevigil, bing, bingapi, brave, bufferoverun, censys, certspotter, criminalip, crtsh, dehashed, dnsdumpster,
                        duckduckgo, fullhunt, github-code, hackertarget, hunter, hunterhow, intelx, netlas, onyphe, otx, pentesttools,
                        projectdiscovery, rapiddns, rocketreach, securityTrails, sitedossier, subdomaincenter, subdomainfinder99,
                        threatminer, tomba, urlscan, virustotal, yahoo, whoisxml, zoomeye, venacus

root@kali:~/home/kali#
```

1.Targethacker

```

root@kali: ~/home/kali
# theHarvester -d gndec.ac.in -b hackertarget
Read proxies.yaml from /etc/theHarvester/proxies.yaml
*****
*                               *
* [H] [A] [V] [E] [S] [T] [I] [N] [G] [I] [N] [G] [I] [N] [G] [I] [N] *
* [H] [A] [V] [E] [S] [T] [I] [N] [G] [I] [N] [G] [I] [N] [G] [I] [N] *
* [H] [A] [V] [E] [S] [T] [I] [N] [G] [I] [N] [G] [I] [N] [G] [I] [N] *
* [H] [A] [V] [E] [S] [T] [I] [N] [G] [I] [N] [G] [I] [N] [G] [I] [N] *
*                               *
* theHarvester 4.8.0                               *
* Coded by Christian Martorella                      *
* Edge-Security Research                            *
* cmartorella@edge-security.com                     *
*                               *
*****

[*] Target: gndec.ac.in

An exception has occurred: Cannot connect to host api.hackertarget.com:443 ssl:<ssl.SSLContext object at 0x7f9a1aa59d00> [Connection refused]
[*] Searching Hackertarget.

[*] No IPs found.

[*] No emails found.

[*] No people found.

[*] Hosts found: 6

mail.gndec.ac.in:103.66.206.61
mail1.gndec.ac.in:175.176.187.101
mail2.gndec.ac.in:175.176.187.102
mail3.gndec.ac.in:175.176.187.103
mx7.gndec.ac.in:175.176.187.107
social.gndec.ac.in:103.66.206.211

```

2.0TX

```
(root@kali)~# cd /home/kali
# theHarvester -d gndec.ac.in -b otx
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

[*] Searching Otx.

[*] IPs found: 30
-----
103.66.206.201
103.66.206.203
103.66.206.204
103.66.206.207
103.66.206.212
103.66.206.214
103.66.206.216
103.66.206.218
103.66.206.219
```

[*] 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

[illegible]