Footprinting and Scanning:

Foundations of Penetration Testing, Identifying Vulnerabilities Before Attackers Do

Presented by RITIKA SHARMA

Introduction to Footprinting & Scanning

Definition:

- Footprinting: Gathering intelligence about a target (e.g., IPs, domains, employees).
- Scanning: Actively probing networks/systems for open ports, services, and vulnerabilities.

Purpose:

- Map attack surfaces.
- Identify weak points before attackers exploit th

Key Tools for Footprinting

Nmap (Network Mapper)

nmap -sV -A testphp.vulnweb.com

Whois/DIG

Retrieves domain registrar and DNS info

Recon-ng

OSINT framework for passive data collection

Shodan/Censys

Search engines for exposed devices

Key Tools for Scanning

Nikto

Web server vulnerability scanner

Dirb/Dirbuster

Bruteforces directories

Netdiscover

Discovers live hosts in local networks

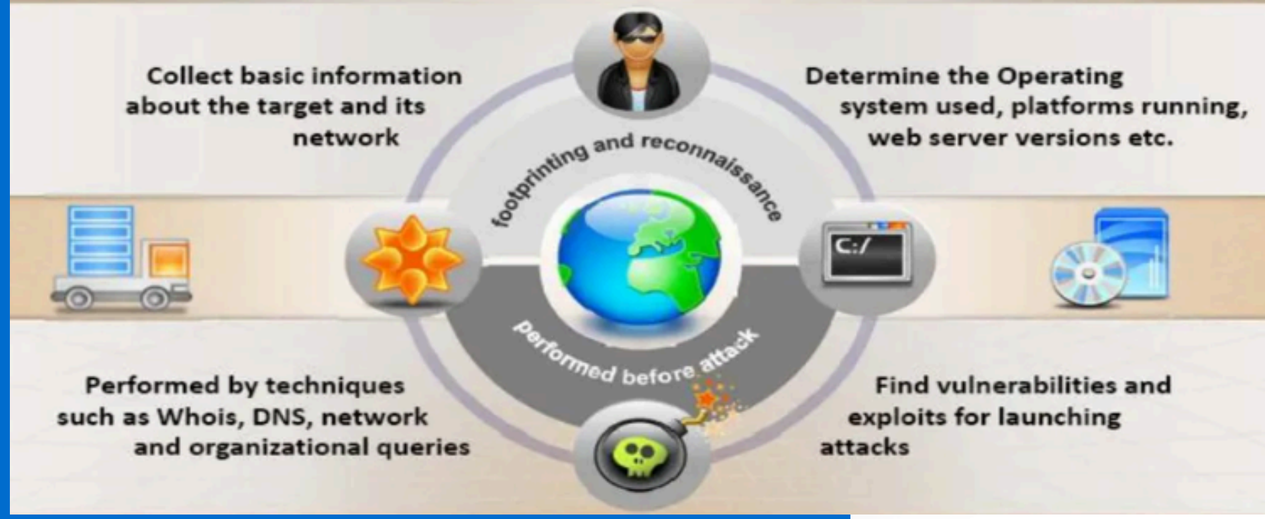
Wireshark

Network protocol analyzer for traffic inspection

Conclusion

Our penetration testing engagement uncovered significant security vulnerabilities through systematic footprinting and scanning. Footprinting activities exposed sensitive organizational data including domain registration details and server geolocations, which could facilitate targeted attacks.

- Footprinting/scanning reveal critical vulnerabilities.
- Tools like Nmap and Nikto automate discovery.



Recommendations

1. Patch Management: Update servers/ software.
2. Firewall Rules: Block unnecessary ports.
3. Input Validation: Sanitize user inputs to prevent SQLi/XSS.