

Internal Recon

Tools and Techniques for Conducting Internal Recon

Identifying Servers, Open Ports, and Services

Port Scanning

Nmap

COMMAND

- nmap -p
- nmap -sV
- nmap -O
- nmap -A
- nmap -sU -p
- nmap -T4 -F

Naabu

ASN Discovry and many more

Amass

Shodan

- search
- host

OSINT

Google Dork

Publicly Exposed Documents	site:example.com filetype:pdf
Directory Listing Vulnerabilities:	site:example.com intitle:"Index of"
Configuration Files Exposed	site:example.com ext:conf OR ext:ini OR ext:config
Database Files Exposed:	site:example.com ext:sql OR ext:db
Log Files Exposed:	site:example.com ext:log
Backup and Old Files:	site:example.com ext:backup OR ext:old
Login Pages:	site:example.com inurl:login
SQL Errors	site:example.com intext:"SQL syntax error"
site:example.com intext:"SQL syntax error"	site:example.com intext:"PHP Parse error" OR intext:"PHP Warning"
Pastebin and GitHub Searches	site:pastebin.com OR site:github.com OR site:gitlab.com

Online Tools

- <https://bgp.he.net/>
- <https://dnsdumpster.com/>

Who Am i

👋 Hello, Hacker! 👋

I'm Matin, an experienced Information Security Analyst with a passion for offensive security. As a bug hunter, I explore vulnerabilities, hunt for security issues, and contribute to the cybersecurity community. You'll often find me participating in CTF (Capture The Flag) challenges on platforms like Hack The Box and TryHackMe.



JavrOOt



Javroot

My social account