Unit 3

▼ Nikto

- Open source, free, web server scanner.
- cross plateform.
- it is perl based scanner, that seraches for common vulnerabilities that can be found on web servers or applications, like dangerous files, outdated system updates, some common misconfiguration.
- although it may not be so helpful when it comes to scan custom web services or application.
- for ex. it may tell you that you’re using outdated version of wordpress, if the website is developed using wordpress, but if we personally wrote the website from scratch then it might not be that great for nikto.
- Looks for over 6500 dangerous files.
- checks for outdated components.
- identifies any misconfigurations.
- attempts to identify vulnerabilities in installed softwares or services.

▼ w3af

- open source, free, web security scanner.
- Stands for Web Application Attack and Audit framework
- it can scan websites for vulnerabilities and performs many kinds of attacks on web application to exploit those vulnerabilities, attacks can be
  - SQL INJECTION
  - XSS
  - Broken authentication.
  - Guessable credentials.
- Cross plateform

- it has both choices, GUI and CLI.
- it can identify more than 200 vulnerabilities and can reduce websites risk exposure.
- written in python & well documented.
- it has plugins that communicates with each other
- we can use following command to open w3af console in terminal
    - ./w3af_console

▼ Curl

- stands for “Client For URLs”
- it can be used to transfer data over network via using many kinds of protocols.
- Curl is a CLI Tool for making/receiving requests/data from network via protocols like HTTPS, FTP etc.
- when HTTPS is specified protocol in Curl command it automatically checks for SSL certificate verification.
- Curl can be used to make Bruteforce attacks or it can replay requests in order to find any vulnerabilities.

▼ openssl

- OpenSSL is a general purpose cryptographic library that provides open-source implementation of the SSL and TLS protocols.
- stops attackers from spoofing website or intermediatory attacks.
- most commonly used.
- provides confidentiality by encryption
- provides integrity by creating identity of web servers or websites.
- HTTPS is possible because of openssl.
- it is open source.
- serving majority of all website.

  - cross plateform
  - Has API & CLI both.

▼ Stunnel

  - openssl supports communication only over HTTPS, Communication in HTTP is not allowed so if a situation exist where a client have to respond back something and client can not communicate directly over HTTPS, then we can not downgrade the communication to HTTP. so in this situation Stunnel comes and when client sends data in PLAIN TEXT format Stunnel will take this data and it will perform encryption in it. so that it will be secure throughout the pathway to destination, and at server side They Stunnel will decrypt the data before sending it to service.
  - Stunnel creation is depended on openssl
  - both machines client & server should have Stunnel installed in their machines in order to communicate over HTTP Stunnel.
  - open source.
  - uses openssl cryptographic library so every algorithm in openssl is supported by stunnel.
  - cross plateform.
  - we can make existing system more secure without modifying original service.

▼ ZED Attack Proxy

ZED Attack Proxy (ZAP) is a free and open-source security tool designed for testing the security of web applications

  - **Acts as a Middleman:** ZAP sits between your browser and the website you're testing. It watches all the communication happening between them.
  - **Finds Weak Spots:** It scans the website for common vulnerabilities like weak passwords, open doors (unsecured endpoints), or places where hackers could sneak in.
  - **Automates and Customizes Testing:** You can use it to automatically check for problems or customize tests for specific scenarios.

- **User-Friendly:** Even though it's powerful, ZAP is designed to be beginner-friendly. It has a graphical interface that makes it easier for people with less technical knowledge to use.
- Internationalized
- cross plateform
- easy to use
- Fully documented.
- Written in java so JDK is required.

▼ SQL map

- Open source, penetration testing tool
- Automates SQL injection attacks with various queries that might give access of database to attacker.
- Can be used to bypass the firewall.
- Supports SQL, MYSQL, ORACLE SQL, POSTGRE SQL, SQLite, MICROSOFT SQL,
- Can crack the passwords which are in hash formats , by dictionary-based attack.

▼ DVWA

- Stands for **Damn Vulnerable Web Application**
- It's a Website which is Very suspectible with many kinds of vulnerability, it is purposefully made for practicing Web scanning and vulnerability scanning.
- It is available so that individual's can test their skills in vulnerability testing & exploiting in a legal way.
- it shows how attackers attack and how we can stop them.
- We can even choose difficulty levels for testing our skills or attacks.
- it contains Following vulns:

    - SQL injection
    - XSS(cross site scripting)
    - Brute force password attacks.
  - It is made in PHP, so that we can even get access to phpmyadmin database via SQL injection.

- ▼ WebGoat
  - Delibarately insecure website , designed to teach people how hackers can attack web sites and how to stop them.
  - it's like a cyber security course, it provides interactive practice.
  - it has lessons about various attacks like SQL INJECTION, XSS, Breaking Authentication.
  - it is java based.
  - goal is to make people aware about various attacks on website so that they can protect their websites better.
  -

- ▼ John the Ripper
  - Free password cracking tool
  - one of the most fastest and Most popular pass cracking tool.
  - primarily used to detect weak UNIX passwords.
  - initially it was only for unix systems, but now it supports more than 15 plateforms.
  - it uses Bruteforce & Dictionary-based attacks, it can auto detect hash types, and combines a number of crackers to do the job fast, it also includes customized cracker.
  - it supports near about 150 hashing algorithms.

- it recognizes common password formats from Some OS files like temp, etc.
    - it keeps track of all the passwords cracked by it in John.pot file.

▼ L0pht crack

- It is password auditing & recovery application.
- used to test password strength & sometimes recovers lost microsoft windows passwords, by using dictionary attacks, bruteforce attacks, hybrid attacks and rainbow tables.
- one of the best tools.

▼ PWDUMP

- it is a tool that can dump or extract password hashes from windows os.
- Security professionals use this tool to check how safe their password hases are.
- if someone dumps hashes using this tool then they can use those hases later to exploit passwords by using tools like L0pht Crack.
- it extracts hashes from Windows Security Accounts Manager (SAM) database, where all the passwords are listed in scrambled format.

▼ THC-HYDRA

- THC Hydra is known for its ability to crack passwords of network authentications by performing brute-force attacks.
- Can perform Rapid dictionary attacks against more than 50 protocols like Telnet, Http, Https, ftp.
- cross plateform

- THC-Hydra is one of the best tool for bruteforcing password attacks, and there are 2 reasons for this.
    - It is fast
    - it can target authentication mechanisms for several protocols.
- When we need to perform bruteforce attacks on remote systems and THC-HYDRA can be a good choice.