18124011600l
Vishwas Acharya

CS

Assignment-5

Date: Page: 1

Q.1) Explain Brute Force Attack in detail.

Ans A brute force attack, also known as an executive search, is a cryptographic hack that relies on guessing possible combination of a targeted password until the correct password is discovered.

- The longer the password, the more combination that will need to be tested.
- It can be time consuming, difficult to perform if methods such as date obfuscation are used, & it times down right impossible.
- However, if the password is weak it could merely take, seconds with hardly any effort.
- It is usually used to obtain personal information such as password, para phrase, username & Personal Identification numbers (PINs), & use a script, hacking application or similar process to carry out a string of continuous attempts to get the information required.

- GOALS of a brute force attack include:

- Harvesting credentials to sell to third parties.
- Theft of personal information.
- Posing as users to send phishing texts or spread fake content.

- Redirecting domains to sites holding malicious content.

- **Brut Force Attack Tools** : An attacker is usually aided by automated s/w that uses computing to systematically check password combination until the correct one is identified.
  - Tools include Aircracking, John the ripper, lophtcrack, Rainbow crack.

- **Types of Brut Force Attack** :

(i) Hybrid Brut Force Attacks
(ii) Reverse Brut Force Attacks
(iii) Credential stuffing

Q.26 What are the password cracking tools? Explain these tools in detail?

Ans - In cryptoanalysis & computer security, it is the process of recovering passwords from data that has been stored in or transmitted by a computer system.
- It is well-designed password-based authentication system doesn't store a user's actual password.
- This would make it far too ~~eee~~ easy for a hacker or a malicious insider to gain access to all ~~of~~ ~~e~~ the user accounts on the system.

- The most commonly used password-cracking tools:

(i) Hashcat :- It is one of the most popular & widely used password crackers in existence. It is available on every OS & supports over 200 different types of hashes.

(ii) John the Ripper :- It is a well-known free open source password cracking tool for Linux, Unix & Mac OS X. A window version is also available.
- It offers password cracking for a variety of different password types.
- It goes beyond OS password to include common web apps (wordpress), compsehend archievs, decurmed files & more.

(iii) Aircrack-ng :- It is a wifi password cracking tool that can crack WEP or WPA/WPA 2 PSK passwords.
- It analyzes wireless encrypted packets & then tries to crack passwords via the dictionary attacks & the PTW, FMS & other cracking algorithms.

(iv) Rainbow Crack :- All password cracking is subject to a time-memory trade off.
- It an attacker has pre-computed a

table of password/hash pairs & stored them as a "rainbow table" then the password cracking is simplified to a table lookup.

- It is a password cracking tool designed to work using rainbow tables.
- It is possible to generate ~~autho~~ custom rainbow tables or take advantage of pre-existing ones downloaded from the internet.

(v) Medusa :- It is an online password cracking tool similar to THC Hydra.

- It claims to be a speedy, parallel, modular & login brute-forcing tool.

(vi) Wfuzz :- It is a web application password cracking tool like brute that tries to crack password via a brute-force guessing attack.

- key feature of it
  - ↳ cookie fuzzing
  - ↳ Output in colored HTML
  - ↳ Multi threadding

- THC Hydra, Oph crack, Lopht crack, Brutes etc. tools

Q.3) Write a notes on

(A) Open SSL and Open SSH :-

- Open SSL is a sobust, commercial grade & full featured toolkit for the transpost layes security and SSL protocols.
  - ↳ It is also a general purpose cryptography libsary
  - ↳ Alibaba Group, GrubHub, Godaddy and othes companies use OpenSSL.
  - ↳ Linux, Windows, Andsoid OS, MAC OS X tools are integrate with open SSL
- Open SSL is a software library for application that secure communications over computes netwoks against eavesdropping or need to identify the party at the othes end,
- It is widely used by Internenet sevsers, including the majority of HTTPS websites.
- OpenSSH is the premies connectivity tool for semote login with the SSH protocol
  - ↳ It encrypts all traffic to eliminate eavesdropping, connection, hijacking & othes attacks.
  - ↳ In addition, OpenSSH provides a large suite of secure tunneling capabilities, several authentication methods & sophisticated configuration options.

↳ Bitbucket, ELCA Vietnam, Chartio, Smarter Agent Mobile companies used open SSH

↳ Linux, Free BSD, MAC OS X, open BSD tools integrate with open SSH.

- Open SSH is also known as open BSD secure shell.
- It is a suite of secure networking utilities based on the SSH protocol, which provides a secure channel over an unsecured network in a client-server architecture

[B] Stunnel:- It is an open-source multi-platform application used to provide a universal TLS/SSL tunneling service.

- It can be used to provide secure encrypted connections for clients or servers that do not speak TLS or SSL natively.
- It runs on a variety of OS, includes most Unix-like OS & windows
- Stunnel relies on the open SSL library to implement the underlying TLS or SSL protocol.
- It uses public-key cryptography with x.509 digital certificates to secure the SSL connection & clients can optionally be authenticated via a certificate

- It is maintained by Michal Trojnara & released under the terms of the GNU General public Licence (GPL) with openssl exception.

[C] HTTP (url) :- It is computes software project providing a library & command-line tool (curl) for transferring data using various network protocols.

- cURL is a command-line tool for getting or sending data including files using URL syntax.
- Since URL uses ~~libcurl~~ libcurl, it supports every protocol libcurl supports.
- cURL supports HTTPS & performs SSL certificate verification by default when a secure protocol is specified such as HTTPS.
- There are many several options to specify a CA certificate such as:
  --cacert and --capath
- In the windows platform, if a CA certificate file is not specified, cURL will look for a CA certificate file name "curl-ca-bundle-crt" in the following orders.

1. Directory where the cURL program is located.
2. Current working directory.

3. Windows system directory
4. Windows directory
5. Directories specified in the % PATH % environment variables.

- It supports numerous protocols as put in URL terms : schems DICT, FILE, FTP, GOPHER, HTTP(S), IMAP(S) LDAP(S), MQIT, POP3, RTMP, RTSP, SCP, SFTP, SMTP, TELNET, TFTP.
- CURL normally displays a progress meter during operation, indicating the amount of transformed data, transfer speeds & estimated time left, etc.

Q.4b What are the application inspection tools? Explain these tools in details?
[zed Attack Proxy, sqlmap, DVMA, webgoat]

Ans It is encompasses measures taken to improve the security of an application often by finding, fixing & preventing security vulnerabilities.
- Different techniques are used to surface such security vulnerabilities at different stages of an applications lifecycle such as design development, deployment, upgrade, maintenance.

- WWW has become a powerful platform for application delivery.
- Sensitive data increasingly made available through web applications.

- **Zed - Attack Proxy:** It is penetration testing tool for finding vulneabilities in web applications
  - It can be used by people with a wide range of security experience
  - Ideal for new developers & functional testers who are new to penetration testing.
  - In addition it useful to an experienced pen testers toolbar.
  - It is released on september 2010

ZAP Principles	Features of ZAP
- Free, open source	- Intercepting proxy
- cross platform	Automated scanner
- Easy to use	passive scanner
- Easy to install	Brute force scanner
- Internationalized	spider, Fuzzer
- Fully documented	port scanner
- Reuse well regarded components	Dynamic SSL certificate

- **Functioning of ZAP :-**
  - ↳ Reposting
  - ↳ Analysing the scan results
  - ↳ Automated scanner
  - ↳ Traditional & AJAX spiders
  - ↳ Intescepting the traffic

- others feature of ZAP are port scan, Encode - Decode Hash, Fuzzing & Extension fo ZAP

- **SQLMAP :** It SQL injection tool used to performing automated injection in database & try to fetch tables out of it.
- SQL map used by whitehat & Blackhat hackers.
- Blackhat try to exploit random os targeted sites using this tool as a challenge os harming sites.
- while white-hat hackers use that tool for scanning their client's websites for any injectable query if they found they respect to administos & get bug bounty os easy reward from it.
- SQL map tests whether a 'GET' parameter is vulnerable to SQL Injection

- Prevention of SQL Injection :-
  - ↳ Reduce the attack surface
  - ↳ Use bind argument
  - ↳ Filter & sanitize input
  - ↳ Avoid dynamic SQL with concatenated input.

- **DVWA :-** It is stand for Damn vulnerable web application.

- It is a PHP/MySQL web application that is a damm vulnerable
- Its main goals are to be an aid for security professionalics do test their skills & tools in a legal environment, helps web developers bettes understand the processes of security web apps. & aid teacher/student to teach/learn web application security in a class room environment

- **Webgoat** :- It is deliberately insecure web application maintained by OWASAD designed to teach web application security lessons.
- This program is a demonstation of common secure side application flaws

NOTE:- while running this program your machine will be extremely vulnerable to attack.

- Web application security is difficult to learn & practice
- Not many people have full blown web apps. like online book stores or online book that can be used to scan for vulnerabilities.
- In addition, security professionals frequently need to test tools against a platform known to be vulnerable do ensure that they perform as advertised
- All of this needs to happen in a safe & legal environment.